Proposal of C4MS and inherent technical challenges – D3.1

Project Number:	ICT-2009-257385
Project Title:	Opportunistic networks and Cognitive Management Systems for Efficient Application Provision in the Future Internet - OneFIT
Document Type:	Deliverable

Contractual Date of Delivery:	31.03.2011
Actual Date of Delivery:	31.03.2011
Editors:	M. Filo
Participants:	See contributors' table
Workpackage:	WP3
Nature:	PU[1]
Version:	1.0
Total Number of Pages:	95
File:	OneFIT_D3.1_20110331

Abstract

The scope of OneFIT is on Opportunistic networks and Cognitive Management Systems for Efficient Application Provision in the Future Internet. This document contains a proposal of Control Channels for Coordination of Cognitive Management Systems (C4MS) which enables delivery of guidance/assistance information from infrastructure towards the Opportunistic Networks and provides means for the management of Opportunistic Networks. This document defines first messages and elementary procedures for the C4MS as well as it identifies a preliminary set of information which is to be conveyed over C4MS. The document introduces also the inherent technical challenges related to the C4MS proposal.

Keywords List

Control Channels for Coordination of Cognitive Management Systems, C4MS, Opportunistic networks (ON), Parameters, Elementary procedures and messages, Inherent technical challenges, Implementation options

[1] Dissemination level codes: **PU** = Public
PP = Restricted to other programme participants (including the Commission Services)
RE = Restricted to a group specified by the consortium (including the Commission Services)
CO = Confidential, only for members of the consortium (including the Commission Services)

Executive Summary

The OneFIT project [1] is a collaborative research project which aims to design and validate the concept of opportunistic networks (ONs) coordinated by the infrastructure. The solutions proposed within the project are foreseen to provide enhanced wireless service provision and extended access capabilities for the Future Internet era.

This document presents a proposal of the Control Channels for the Cooperation of Cognitive Management Systems (C4MS) which enables delivery of guidance/assistance information from infrastructure towards the Opportunistic Networks and provides means for the management of Opportunistic Networks. The information exchanged over C4MS is necessary for the realization of suitability determination, creation, maintenance and termination of Opportunistic Networks.

The first sections of the document provide an introduction to the main C4MS concept and define C4MS requirements which have been derived based on the system requirements developed in D2.1 [2]. The C4MS is introduced as a combination and evolution of the Cognitive Pilot Channel (CPC) and the Cognitive Control Channel (CCC) concepts.

Section 3 includes a review of the Functional Architecture (FA) and the System Architecture (SA) developed in D2.2 [3]. The section depicts also the projection of C4MS onto the OneFIT system architecture, indicating different possible logical connections between Cognitive Management Systems which needs to be handled by the C4MS.

Based on the technical challenges identified in D2.1 [2], the first set of parameters/information to be exchanged between different cognitive managements systems over C4MS is derived in Section 4. The identified set was determined as necessary to enable the operation of mechanisms in different ON phases and is to be further updated in the future work. The information/parameters are categorized based on the type of the technical challenges it originated from.

Section 5 goes into more detail regarding the C4MS. The C4MS can be considered as an intermediate layer between C4MS users and the network protocol stack. The main role of C4MS is to enable and coordinate the exchange of information between C4MS users located in different nodes. In this section, different C4MS services including information delivery, message relaying, and security are briefly discussed and an initial set of elementary procedures and related messages for the C4MS protocol are introduced based on the Message Sequence Charts proposed in D2.2 [3]. Several different procedures along with the messages necessary to conduct these procedures are specified in this section (the messages are specified using the ABNF specification). The section encompasses also description of possible C4MS implementation options indentified based on different existing protocols and systems. The options have been subdivided into two groups: RAT/System independent (e.g. IETF Diameter, IEEE 802.21, 3GPP ANDSF) and RAT/System dependent (e.g. 3GPP, 802.11, WiMedia, Bluetooth).

The document continues with the elaboration on the technical challenges derived based on the introduced C4MS proposal in Section 6. The technical challenges are related to different aspects such as standardization and deployment of the C4MS within the existing systems.

Finally the conclusions are drawn in Section 7 and state of the art in the context of C4MS is presented in the Appendix A.

Contributors

First Name	Last Name	Affiliation	Email
Jens	Gebert	ALUD	Jens.Gebert@alcatel-lucent.com
Marcin	Filo	EIT+	marcin.filo@eitplus.pl
Krystian	Sroka	EIT+	Krystian.sroka@eitplus.pl
Markus	Mück	IMC	markus.mueck@intel.com
Andreas	Schmidt	IMC	andreas.schmidt@intel.com
Benoit	Lécroart	NTUK	Benoit.lecroart@nectech.fr
Christian	Mouton	NTUK	Christian.mouton@nectech.fr
Lanto	Rakotoharison	NTUK	Lanto.Rakotoharison@nectech.fr
Oscar	Moreno	TID	omj@tid.es
Seiamak	Vahid	UNIS	S.Vahid@surrey.ac.uk
Ramon	Ferrús	UPC	ferrus@tsc.upc.edu
Oriol	Sallent	UPC	sallent@tsc.upc.edu
Panagiotis	Demestichas	UPRC	pdemest@unipi.gr
Andreas	Georgakopoulos	UPRC	andgeorg@unipi.gr
Nikos	Koutsouris	UPRC	nkouts@unipi.gr
Vera	Stavroulaki	UPRC	veras@unipi.gr
Kostas	Tsagkaris	UPRC	ktsagk@unipi.gr
Marja	Matinmikko	VTT	marja.matinmikko@vtt.fi
Miia	Mustonen	VTT	miia.mustonen@vtt.fi
Heli	Sarvanko	VTT	heli.sarvanko@vtt.fi

Table of Acronyms

Acronym	Meaning
3GPP	3rd Generation Partnership Project
ABNF	Augmented Backus–Naur Form
ACL	Agent Communication Language
ANDSF	Access Network Discovery and Selection Function
AVP	Address Value Pair
C4MS	Control Channels for Coordination of Cognitive Management Systems
CCC	Cognitive Control Channel
CCR	Cognitive Control Radio
CMON	Cognitive systems for Managing the Opportunistic Network
CPC	Cognitive Pilot Channel
CSCI	Cognitive management Systems for Coordinating the Infrastructure
DM	Device Management
FIPA	Foundation for Intelligent Physical Agents
HTTP	Hypertext Transfer Protocol HTTP
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers
IEFT	Internet Engineering Task Force
IIOP	Internet Inter-object request broker Protocol
IMTP	Internal Message Transport Protocol
INA	Information Answer
INR	Information Request
Leap	Lightweight Extensible Agent Platform
LTE	Long Term Evolution
MAC	Media Access Control
MIIS	Media Independent Information Service
MSC	Message Sequence Chart
MTP	Message Transport Protocol
OMA	Open Mobile Alliance
ON	Opportunistic Network
ONCA	ON Creation Answer
ONCR	ON Creation Request
OneFIT	Opportunistic networks and Cognitive Management Systems for

	Efficient Application Provision in the Future InterneT
ONMA	ON Modification Answer
ONMR	ON Modification Request
ONNA	ON Negotiation Answer
ONNR	ON Negotiation Request
ONRA	ON Release Answer
ONRR	ON Release Request
ONSI	ON Suitability Indication
ONSN	ON Status Notification
PDU	Protocol Data Unit
RAT	Radio Access Technology
RMI	Remote Method Invocation
SAP	Service Access Point
UE	User Terminal
UWB	Ultra Wide Band
WLAN	Wireless Local Area Network

Table of Contents

List of Figures

List of Tables

1. Introduction

During different phases of Opportunistic Networks (ONs) – the suitability determination, creation, maintenance and termination – control information needs to be exchanged between the involved nodes. For enabling such an exchange of information, the OneFIT project will develop and use the "Control Channels for the Cooperation of the Cognitive Management Systems"(C4MS). The C4MS enables provision of globally and locally valid cognitive information between the nodes of ONs and allows the management of opportunistic networks.

The C4MS comprises both Cognitive Pilot Channel (CPC) [31] and the Cognitive Control Channel (CCC) [43] concepts. The CPC provides information from the network to the terminals on e.g. frequency bands, available Radio Access Technologies and spectrum usage policies and by doing this it acts as a basis for the coordination between infrastructure and opportunistic networks. The CCC on the other hand facilitates information exchange between heterogeneous network nodes (e.g. between terminals). A C4MS common framework will integrate these concepts in the sense that C4MS is able to manage the provision of context information, policies, parameters etc. either between heterogeneous network nodes (terminals or infrastructure nodes) or between terminals and infrastructure, as illustrated in Figure 1.

Figure 1: C4MS – general view.

The context information can be used for supporting terminals in their start-up phase, supporting spectrum scanning and spectrum sensing procedures as well as for enabling the coexistence and coordination between networks and devices. In addition, C4MS extends the CPC and CCC concepts by enabling the management of Opportunistic Networks. It integrates different existing mechanisms for the information delivery and introduces new procedures, and related protocols to enable new features related to Opportunistic Network management.

ONs should be capable to operate dynamically as a part of an infrastructure without interfering with other traffic and operation in the infrastructure. In addition, it should be able to extend the resources and capabilities of the infastructure by utilizing excisting resources in the network as efficiently as possible. For these reasons, nodes have to be able to provide information such as policies, resources, node capabilities (e.g. supported RATs), environment (e.g. available spectrum bands) to each other. In this document, parameters and information to be exchanged between cognitive management systems in order to enable suitability determination, creation, maintenance and termination of ONs are examined in detail. In order to distribute this information to relevant nodes and to avoid excess signaling, efficient information provisioning procedures and their messages are introduced. There are several implementation options for C4MS which can be divided in system/RAT independent and system/RAT dependent options.

The rest of this document is organized as follows. Chapter 2 derives C4MS requirements, based on the system requirements delivered in D2.1 [2]. In Chapter3, an overview of the OneFIT functional and system architecture developed in WP2 is provided. The work of WP 2 is extended by providing the projection of C4MS on the OneFIT system architecture. Parameters and information to be exchanged between nodes are identified and described in Chapter4. Chapter5 introduces C4MS elementary procedures and further elaborates messages needed to exchange information between nodes. It also introduces implementation options for C4MS. Chapter6 addresses specific technical challenges related to the implementation of the C4MS on the existing devices/infrastructure. Finally, conclusions are drawn in Chapter 7.

2. C4MS related system requirements

The following section derives C4MS requirements based on the system requirements developed within WP2. The derived C4MS requirements shall be used to guide the work related to the design and specification of C4MS in WP3.

Requirement C4MS1: Communication with the infrastructure

The C4MS shall allow terminals to directly or indirectly communicate with the infrastructure.

Requirement C4MS2: Communication between terminals

The C4MS shall allow terminals to directly or indirectly communicate with each other.

Requirement C4MS3: Versatile RAT/RAN use

The C4MS shall be usable for different types of radio access technologies to enable operation of different types of homogeneous as well as heterogeneous opportunistic networks. The C4MS should therefore provide radio technology independent mechanisms. However, radio technology intrinsic mechanism e.g. to broadcast certain information may also be supported.

Requirement C4MS4: Mobility

The C4MS needs to be robust also during user mobility within an ON. This means that the C4MS should be robust against packet errors, node disappearance, etc. The C4MSshould therefore allow reliable transfer of information.

Requirement C4MS5: Relaying

The C4MS shall allow forwarding of ON relevant signalling messages. The forwarding capabilities shall be provided for homogeneous as well as heterogeneous networks.

Requirement C4MS6: Opportunistic Network management

The C4MS shall provide communication means to enable the realization of the management procedures related to: ON suitability determination, ON creation, ON maintenance and ON termination (this includes enabling on-the-fly negotiations and agreements).

Requirement C4MS7: Opportunistic Networks controllable by single operator

C4MS shall provide means for the exchange of ON relevant signalling within a network of a single operator. Providing means for the exchange of ON relevant signalling between the operators may optionally be supported.

Requirement C4MS8: Preservation of legacy RAN operation

The impact of C4MS on the legacy RAN operation shall be minimized. The C4MS shall minimize the impact on the “anchor” network, in terms of mobility (idle and connected), spectrum use, security/privacy, charging/billing.

Requirement C4MS9: Compatibility with legacy RAN deployments

The impact of C4MS on the RAN deployments shall be minimized. The C4MS deployment should remain compatible with legacy and foreseeable RAN deployments/planning techniques, e.g. overlays of macro/femto/relay.

Requirement C4MS10:C4MS usage

The C4MS shall enable the exchange of ON relevant signalling between nodes belonging to a single opportunistic network.

The C4MS shall enable the exchange of ON relevant signalling between nodes belonging to different opportunistic networks.

The C4MS shall enable the exchange of limited ON relevant signalling between nodes which are candidates for the ON.

Requirement C4MS11: C4MS information

The C4MS shall support the exchange of different type of information relevant for the ON management. This includes: context information, policies, decisions as well as pure signalling data.

The information shall be encoded compactly to minimize the signalling load.

Requirement C4MS12: Broadcast/Multicast

The C4MS shall support mechanisms to transmit information to several nodes, e.g. via broadcast or multicast mechanisms.

Requirement C4MS13: Unicast/Dedicated addressing

The C4MS shall support mechanisms to transmit information to a single node identified via an address, e.g. via unicast or dedicated mechanisms.

Such a peer-to-peer connectivity shall be supported also in cases without the existence of a direct link between the two communicating nodes (forwarding of signalling data shall be possible).

RequirementC4MS14: Secure as well as unsecure communication

The C4MS shall allow for unsecured as well as secure data transmission, dependent on the confidentiality of the data.

Requirement C4MS15: C4MS efficiency

The amount of signalling shall be minimized.

The latency shall be compatible with targeted applications' requirements for QoS, even if several hops are involved.

RequirementC4MS16: Implementation

The reuse of existing protocols should be considered. Open, extensible protocols are preferred.

The C4MS shall be capable of supporting several simultaneous signalling transactions per node.

3. OneFIT architecture overview

The following section provides an overview of the OneFIT functional and system architecture developed in WP2. Additionally, it provides the projection of C4MS on the OneFIT system architecture.

3.1 Functional architecture

As defined in D2.2 [3], the functional architecture (FA) proposed within the OneFIT project is an extension of the functional architecture for the management and control of reconfigurable radio systems as defined in the ETSI TR 102 682 [32]. The proposed extension enables infrastructure goverened Opportunistic Network Management and it consists of two building blocks:

- "Cognitive management System for the Coordination of the infrastructure" (CSCI) and
- "Cognitive Management system for the Opportunistic Network" (CMON).

The basic funtionalities as well as their split between the proposed blocks have been defined in [3] and can be seen in Table 1.

	CSCI	**CMON**
Coordination with the Infrastructure (Infrastructure not necessarily part of the ON)	YES	-
Coordination with other nodes in the ON	-	YES
Detection of situations where an ON may be useful	YES, typically based on external triggers, e.g. information from JRRM	-
ON Suitability determination	YES	-
Execution of ON establishment/creation	-	YES
Maintenance of ON, e.g. reconfiguration	-	YES
Decision on termination of ON when ON is no longer suitable	-	YES, typically based on external triggers
Execution of ON termination	-	YES

Table 1: Functionalities of CSCI and CMON [3].

The following figures depict the localization of the proposed OneFIT functional entities and present OneFIT interfaces for two possible Opportunistic Network configurations. In the first configuration shown in Figure 2, the infrastructure of an operator is always part of the ON whereas in the second configuration, in Figure 3, the interface is not part of the ON but only provides assistance.

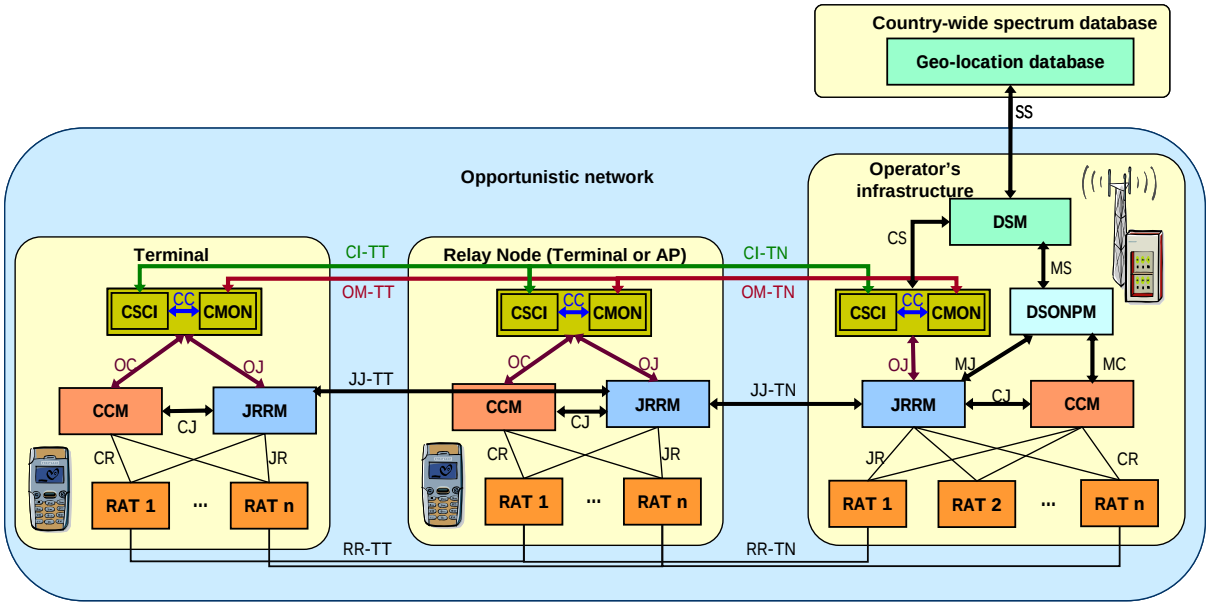


Figure 2: OneFIT Functional Architecture for the Management and Control of infrastructure governed Opportunistic Networks[32]

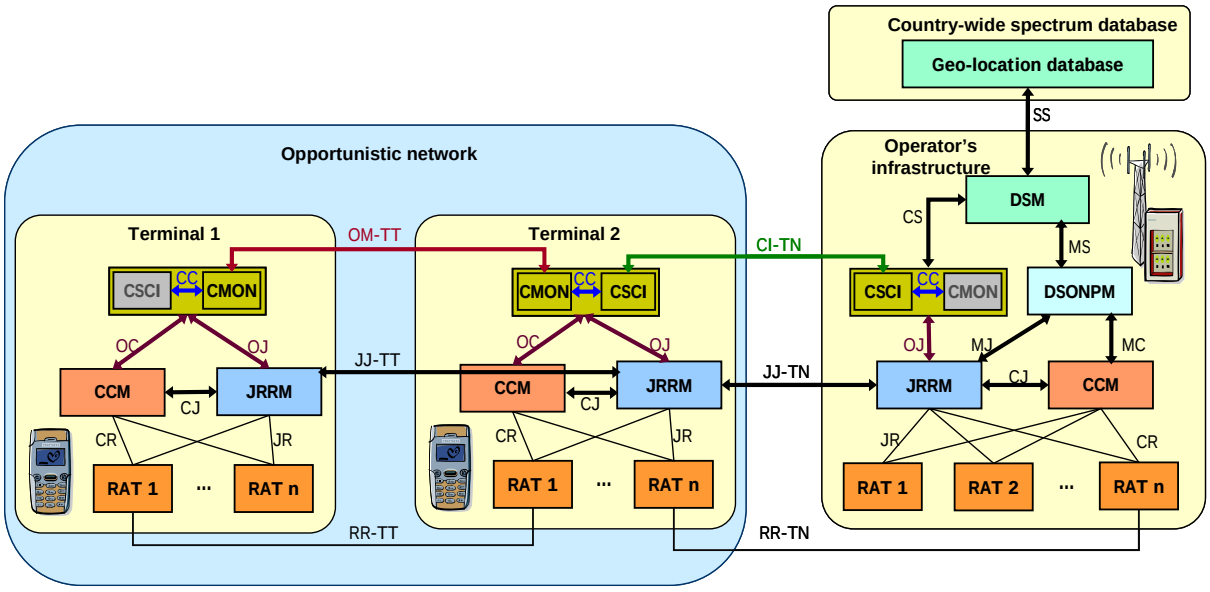


Figure 3: OneFIT Functional Architecture example where the infrastructure is not part of the ON

The figures above show the following interfaces of the OneFIT Functional Architecture:

- The CI-Interface for "Coordinating the Infrastructure" located between different CSCI-instances. The CI-interface can connect the CSCI-instances of two terminals (CI-TT), the CSCI in a terminal with the CSCI on Network side (CI-TN) or the CSCI-instances of two network entities (CI-NN).
    - CI-TN – the interface is used for collecting context information from the terminals to enable the ON suitability determination. The operator can either request the necessary context information or set conditions for the "CSCI-T context information push".The interface also allows CSCI-T to register with

CSCI-N. In case the strict operator supervision over ONs is not necessary (i.e. no CMON-N), the interface can be used to inform CSIC-T about the need of ON creation (ON creation trigger);

- CI-NN - the interface is used for enabling the coordination of resource allocation to multiple ONs and support ON merging/splitting, it can also be used for ON suitability determination and creation in the case of ON formed by infrastructure nodes;
- CI-TT – the interface is used for extending interface CI-TN in the situation in which a terminal does not have a direct access to CSCI-N. The interface allows CSCI-T to register with CSCI-N via other CSCI-T.

- The OM-Interface for the "Opportunistic Management" located between different CMON-instances. The OM-Interface can connect the CMON-instances of two terminals (OM-TT), the CMON in a terminal with the CMON on Network side (OM-TN) or the CMON-instances of two network entities (OM-NN):
  - OM-TT – the interface enables the coordination and cooperation of terminals during creation, maintenance and release of ON. by allowing the exchange of context information, policies, profiles, decisions;
  - OM-TN – the interface enables the supervision of operators over ONs by allowing the operator to reconfigure ON, request measurements and push and pull context information from CMON-T;
  - OM-NN – the interface enables the coordination and cooperation of Network entities during creation, maintenance and release of ONby allowing the exchange of context information, policies, profiles, decisions.
- The CC-Interface connecting the CSCI and the CMON inside one node e.g. for sending a trigger for the creation of an ON from the CSCI to the CMON or for providing information about the resources available for the ON.
- The CS-Interface located between CSCI/CMON and the Dynamic Spectrum Management (DSM) and which can be used for obtaining information on spectrum usage and spectrum policies from the DSM.
- The OJ- Interface located between the CSCI/CMON and the Joint Radio Resource Management (JRRM). The CSCI and CMON are assumed to use the same protocol or API to exchange information with the JRRM. The OJ-Interface can connect the CMON/CSCI instances with JRRM in a terminal (OJ-T)or on Network side (OJ-N)
  - OJ-T –enables the collection of local context information (e.g. available access networks in the neighbourhood, channel conditions, device location) to determine the suitability of ONs (CSCI).). It also enables efficient management of resources for creation, maintenance and release of ONs (CMON);
  - OJ-N – enables the collection of global context information (e.g. number of device in different cells, cell loads, and interference levels) to determine the

suitability of ONs (CSCI). Itis also relevant for creation, maintenance and release of ONs (CMON).

- The OC- Interface located between the CSCI/CMON and the Configuration Control Module (CCM). Similarly to the OJ interface, both CSCI and CMON use the same interface to communicate with the CCM. The interface can be used for obtaining information about the current device configuration or instructing the CCM to execute a reconfiguration.

3.2 OneFIT system architecture for C4MS

As defined in [3], the OneFIT system architecture consists of two main building blocks: The Cognitive management systems (CSCI and CMON) and the Control Channels for Coordination and Cooperation of cognitive management systems (C4MS).

The OneFIT cognitive management systems can reside in various elements of an underlying network. The OneFIT system shall also support ONs which may consist of different systems (e.g. 3GPP based systems such as GSM, UMTS or LTE and non-3GPP systems such as WiMax, WiFi, Bluetooth, WiMedia). In order to enable the realization of the ON management and the exchange of context information for such scenarios, the C4MS needs to allow for the establishment of connections (logical or physical) between different entities which reside on the terminal as well as on the infrastructure side, over different underlying technologies.

Figure 4 shows how the OneFIT system elements can be mapped onto existing network entities and depicts different types of C4MS connections. As can be seen from the figure, the C4MS is supported by all the entities which employ CSCI and/or CMON and it can be seen as an intermediate layer residing between CMON/CSCI and the underlying layers. The blue dashed lines represent interfaces between CSCIs of different network nodes (CI) or interfaces between CMONs of different network nodes (OM) (see Section 3.1).

For some scenarios, the C4MS could be optionally supported by the O&M systems in case the network operator is willing to employ its own O&M systems to enable the exchange of C4MS data. This approach would be especially useful for the exchange of data between different systems (see Section 5.4.5 for more detail).

In order to minimize the impact on the existing networks the OneFIT based extensions are proposed to be placed in the Radio Access Network (RAN), leaving the Core Network intact or with minimal changes.

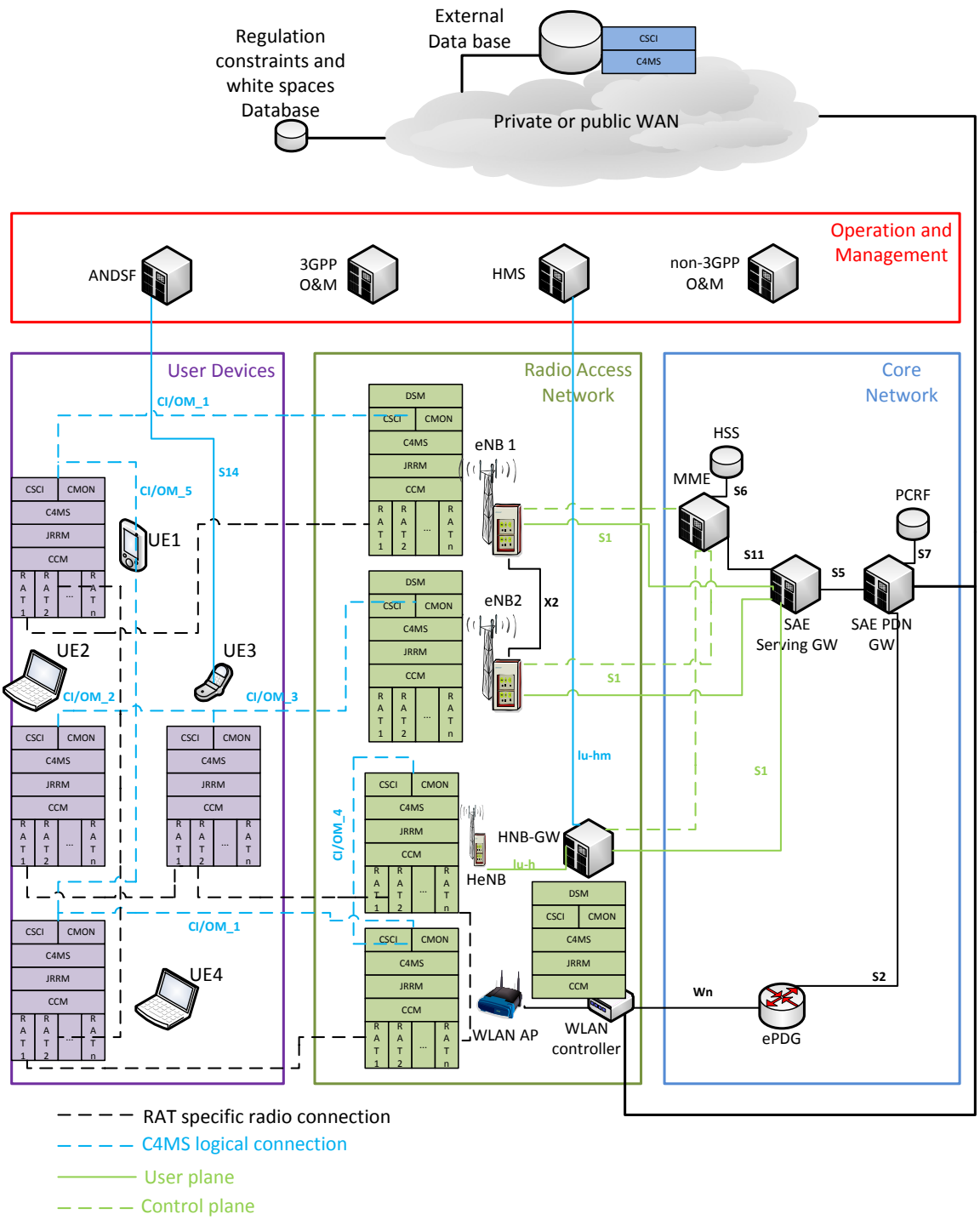


Figure 4: Mapping of the OneFIT system building blocks to the underlying network [3]

4. Information exchanged in the OneFIT system

The following section identifies and describes parameters and information which need to be exchanged for the management of opportunistic networks. The derivation of such information has been done according the key functionalities of the underlying ON operation and not focusing on specific ON procedures which are addressed in section 5.3.

Four phases are distinguished within ON life-cycle: suitability determination, creation, maintenance and termination [2].

The suitability determination phase is needed to decide whether it is suitable to set up an ON at a specific time and place based on the observed radio environment and some established criteria. The suitability assessment is the result of a rough feasibility analysis in order to keep complexity moderate. The functionalities needed to support this phase are node identification, radio path identification and assessment of potential gains. Radio path identification includes spectrum opportunity identification and route identification. As well, a transversal functionality for interference handling is considered to be embedded within node, spectrum and route identification functionalities that already take into account interference issues.

Triggered by a positive outcome of the suitability determination phase, the creation phase will attempt to end up with the final configuration of the ON. Decision-making in this phase is likely to require additional context awareness and/or more accurate estimations related to diverse aspects of the radio environment. Therefore, the same functionalities identified in the suitability determination phase also apply at this phase (i.e. node, spectrum and route selection) although the level of detail of the information to be managed will be different.

Once created, the ON enters in the maintenance phase. An ON will be dynamic in nature during all its operational life-time. Capabilities for the ON's reconfiguration will provide the necessary adaptability to changing conditions. Hence, during this phase, a monitoring functionality is needed to dynamically acquire all the relevant information needed to check that the ON is still valid and efficient for what it was created. According to this information about ON's validity and efficiency, monitoring functionality can trigger reconfiguration or termination functionalities. Reconfiguration functionality will decide on all the appropriate changes at the ON configuration in order to achieve the most efficient operation of the ON. Reconfiguration functionality will actually rely on the same functionalities also supporting the suitability and creation phases (i.e. node, spectrum and routes identification and selection). When the ON operation is no longer necessary or suitable, the ON will be terminated. In this case, functionality for handover to infrastructure handling is also needed to address the case when an ON termination decision is made but some of the services being provided over the ON shall be kept alive over the infrastructure network. Termination may also be forced suddenly due to reasons external to the ON e.g. loss of the spectrum band. Also in this situation there needs to be a mechanism for the ON to handover the service to the infrastructure.

Additionally, security and trust functionalities are also necessary for ON operation in all ON operational phases.

Based on above description, parameters and information to be exchanged have been organised in the remainder of this section attending to the following key functionalities that are to be present across one or several of the ON operational phases:

- Node identification and selection
- Spectrum opportunity identification and selection
- Route identification and selection
- Interference handling
- Monitoring and reconfiguration/termination
- Security and trust

4.1 Node identification and selection

This functionality is intended to identify and select which nodes to participate in an ON. The functionality is needed in the suitability determination phase of an ON (candidate node identification), in the creation phase (node selection) and during the maintenance phase where the composition of the ON may change (identification and selection of new/existing nodes to join/leave the ON).

The following information has been identified as a potential input for candidate node identification and selection mechanisms and thus may need to be exchanged over different ON interfaces. It is worth noting that part of this information may be available over other means than C4MS (e.g. over some RAT specific mechanisms).

- Radio Environment information (information per operator)
    - Spectrum usage map
    - Spectrum usage policies
    - Path loss map
- Policies (information per operator)
    - Intra-operator Inter-system mobility policies
    - Inter-operator mobility policies
- Candidate node database (information per node)
    - Node capabilities
        - Node Class (e.g. Access Point, Mobile Node)
        - Supported RATs:
            - Types of supported technologies (e.g. WiFi, Bluetooth, UMTS)
            - Number of interfaces for each supported technology (in some cases we may have e.g. multiple WiFi interfaces within a single node)
            - Supported Frequency Bands and number of supported channels (for each supported technology)
            - Maximal/Minimal TX power (for each supported technology)
            - QoS capabilities that can be established in terms of:

        - Maximum bitrate(s) supported in kbit/s per traffic direction (uplink, downlink or bothway)
        - Guaranteed bitrate(s) supported in kbit/s per traffic direction (uplink, downlink or bothway)
        - An indicator on which QoS classes are supported (Conversational, Streaming, Interactive, Background)
      - Energy consumption in different power states (for each supported technology)
      - RAT specific transmission capabilities (e.g. carrier aggregation, RAT specific modulation coding schemes)
    - An indicator if relaying of traffic for other nodes is supported
    - An indicator if geo-location is supported
    - An indicator if multiple simultaneous radio links are supported
  - Node policies
    - Billing policy
    - User policies with regard to ON (e.g. minimal battery level when user is willing to relay traffic, preferred type of relayed traffic)
  - Node Context info
    - Status (idle, connected, etc.)
    - Available resources (subcarriers, codes, remaining bit rate, remaining battery capacity, processing and storage capabilities)
    - Established bearers (QoS parameters) per RAT
    - Current/max/mean goodput
    - Current/max/mean delay
    - Fitness value (which provides an indication of the energy level, the delivery probability and the availability of a node)
    - Serving BS
    - Route to serving BS (e.g. direct, through XYZ…)
    - Gateway capability
    - Mobility level (current location, speed, direction)
  - Information related to requesting application(s)
    - Requested bearers/QoS
    - Application characterization (e.g. expected duration, elasticity, etc.)

On the other hand, the following information has been identified to be a potential output of candidate node identification mechanisms and thus may need to be exchanged over different interfaces:

- List of candidate nodes ranked based on the fitness value
    - Node Ids
    - Fitness values

A discovery procedure is a key mechanism used by the node identification functionality. Existing discovery procedure as described in section 5.3.3 may be modified in order to indicate if opportunistic networking is supported by a node or not. It is for further study if discovery messages (broadcast messages, beacons, probe responses) should be extended with additional information like conditions for opportunistic networking or not.

4.2 Spectrum opportunity identification and selection

This functionality is intended to identify available spectrum usable by the ON nodes and to select the most appropriate configuration. This functionality is needed in the suitability determination phase of an ON (spectrum opportunity identification), in the creation phase (spectrum selection) and during the maintenance phase where the composition and configuration of an ON may change (e.g. changes in available spectrum). In case the use of spectrum is based on local information obtained e.g. from other nodes, changes in the availability of the spectrum should be periodically monitored during the maintenance of an ON.

The spectrum opportunity identification mechanisms are responsible for the identification of spectrum available for a transmission in a given area and providing input towards spectrum selection mechanisms. In order to allow the implementation of different types of mechanisms (e.g. centralized, decentralized, cooperative, non-cooperative), different parameters and information needs to be exchanged between ON participants.

Potential inputs to spectrum opportunity identification mechanisms that may be required to be exchanged over different interfaces are the following:

- Information on node capabilities and policies (sets constraints for spectrum opportunity identification mechanisms):
    - Node capabilities related to spectrum opportunity identification:
        - An indicator if a node can conduct spectrum sensing and which sensing techniques it supports (e.g. energy detection, feature detection-based)
        - An indicator if a node can conduct channel measurements
        - Information on the tuneable parameters (supported frequency bands, maximal frequency bandwidth)
    - Policies:
        - Allowed frequency bands and transmission bandwidth
        - Allowed transmission power on different bands
        - Allowed mechanisms to obtain information on the spectrum usage (control channel, data base or spectrum sensing)
- Information used for the configuration of the spectrum sensing or channel measurements:

- Spectrum sensing technique (e.g. energy detection, feature detection) and related parameters (e.g. detection threshold)
- Frequency band(s) to scan
- Time available for spectrum sensing
- How often spectrum sensing should be performed (depends on the interference tolerance of the existing services on different bands)
- Information on the existing services on different bands (e.g. signal type)

- Information used as an input towards the decision engine:
  - Spectrum availability information obtained from the geo-location database and/or from other nodes (in a form of a raw spectrum sensing/channel measurement data or pre-processed data)

It is worth noting that part of above information may be available over other means than C4MS (e.g. over some RAT specific mechanisms).

Furthermore, potential outputs of spectrum opportunity mechanisms that may be required to be exchanged over different ON interfaces are the following:

- Spectrum availability information:
  - Spectrum characterisation (e.g., first and second order spectrum occupancy statistics, grouping of spectrum blocks in spectrum pools with certain similarities)

The spectrum selection functionality will be in charge of deciding which is the spectrum to be used to handle ON communications. Considering as a reference a centralised approach where decision-making was held within CSCI/CMON functional entities on the infrastructure side, information exchange over the different interfaces to be supported over C4MS could be:

- From Terminal to Infrastructure
  - Information related to the application
    - Requested bearers/QoS
    - Application characterization (e.g. expected duration, elasticity, etc.)

    Note: The characterization of applications might be available at the Infrastructure side by other means rather than flowing over CI/OM-TT and CI/OM-TN
  - Information related to the capabilities of the involved Terminals
    - Terminal maximum transmit power
    - Supported frequency bands (e.g. ISM 2.4 GHz, ISM 5 GHz, 900 MHz, ...)
    - Transmission capabilities (e.g. single carrier, carrier aggregation, …)
    - Supported RATs
    - Locations and interconnections

        - Mobility levels

      Note: Terminal's capabilities might be available at the Infrastructure side by other means rather than flowing over CI/OM-TT and CI/OM-TN.

    - Radio interface-related measurements
        - Measured Signal strength
        - Measured Noise and Interference level
        - Measured Propagation losses
        - Measured achieved Bit rate

      Note: The radio interface-related metrics might also be provided by JRRM rather than flowing over CI/OM-TT and CI/OM-TN.

- From Infrastructure to Terminal
    - For each spectrum block forming the selected spectrum pool
        - Central frequency
        - Bandwidth
        - Transmission constraints (maximum transmit power in spectrum block)
        - Estimated availability time e.g. according traffic predictions
        - Policies on different bands
        - Propagation characteristics

4.3 Route identification and selection

The route identification and selection functionality is responsible for the selection of gateway nodes which in some cases interconnect terminals with infrastructure as well as the selection of proper routes between ON participants. This functionality is needed in the suitability determination phase of an ON (determination of potential routes), in the creation phase (route selection) and during the maintenance phase where the composition and configuration of an ON may change (route changes).

In order to allow the implementation of different types of routing protocols or routing selection mechanisms (e.g. centralized, decentralized, on-demand, proactive) different parameters and information needs to be exchanged between ON participants.

Parameters and information which have been identified to be potentially relevant for routing pattern selection mechanisms and thus may need to be exchanged between ON participants are listed in the following.

As to input parameters needed in the node(s) in charge of decision-making, identified information has been sub-divided based on the frequency of its changes as: static and dynamic (or semi-dynamic). It is worth noting that part of this information may be available over other means than C4MS (e.g. over some RAT specific mechanisms).

The static information is used for setting constraints on the routing pattern selection mechanisms and includes mainly node capabilities (see Section 4.1 for the proposed list of node capabilities).

The dynamic or semi-dynamic information is used for determination of different routing metrics and setting optimization goals for routing selection mechanisms:

- Information relevant for determination of different routing metrics:
    - Number of neighbours and their IDs (for each active RAT)
    - Lower layer radio interface dependent measurements (for each neighbouring node and on each active RAT)
        - Measured Propagation loss
        - Measured Noise and Interference level (for each channel)
        - Measured Signal quality (e.g. SINR)
        - Variations of Signal quality
        - Measured PER (Packet Error Rate) and BER (Bit Error Rate)
        - Variations of PER and BER
    - Geographical location (if geo-location is supported)
    - Mobility (to estimate node lifetime as well as link lifetime)
    - Battery drain per second
- Information relevant for determination of a possible optimization goal:
    - Information related to the application:
        - Requested bearers/QoS
        - Application characterization (e.g. expected duration, elasticity, etc.)
    - Battery level

As to output information of routing pattern selection mechanisms that will flow from decision-making nodes to nodes that should enforce such decisions, the following information has been identified:

- Routing tables with information about next hops (for centralized algorithms)
- RAT type(s) to use
- Allocation of frequency channels
- Transmission power
- Maximal bit rate/message rate
- RAT specific configuration (e.g. number of aggregated carriers, id of a specific modulation coding scheme)

4.4 Interference handling

This functionality is a transversal functionality embedded within node, spectrum and route identification and selection functionalities where related decisions already take into account interference issues.

Different approaches can be considered in order to handle the problem of excessive interference within an ON. Depending on the source of interference the following actions may be required:

- In case the source of interference is internal (i.e. a node which is a source of interference is part of an ON), the problem could be solved by decreasing the power of the source or decreasing the message rate of the source. Additionally, some time multiplexing techniques (resource reservation) could be used to decrease (or completely neglect) the overlap between the internal interferers.
- In case the source of interference is external (i.e. a node which is a source of interference is not part of an ON), the problem could be addressed by increasing the coding rate, increasing the transmission power, switching to different frequency band, switching to a different RAT type.

The implementation of the mentioned approaches for interference handling can be conducted in a centralized as well as decentralized way. In case of a centralized implementation the decision-making is held within a single CMON functional entity within an ON (depending on the scenario the interference handling functionality can be located on the infrastructure side or on the terminal side). For a decentralized implementation, the decision making logic is held in every CMONs within an ON.

It is also worth noting that the interference handling functionality requires the implementation of certain mechanisms allowing interference detection. A possible implementation would require monitoring of lower layer quality indicators such as: interference level, signal quality, signal strength and higher layer quality indicators such as: Application QoS.

Information which has been identified to be a potential input of interference handling mechanisms and thus may be required to be exchanged over different interfaces is listed in the following. It is worth noting that part of this information may be available over other means than C4MS (e.g. over some RAT specific mechanisms).

- Information necessary as an input to enable interference detection:
    - Lower layer radio interface dependent measurements
        - Measured Signal strength
        - Measured Noise and Interference level
        - Measured Signal quality (SINR)
        - Measured Propagation losses
        - Measured Packet Error Rate
        - Measured Bit Error Rate
    - Higher layer radio independent measurements

        - achieved Bit rate
        - achieved Goodput
        - mean Bit rate
        - mean Goodput
    - Information related to the application
        - Requested bearers/QoS
        - Application characterization (e.g. expected duration, elasticity, etc.)
- Information necessary as an input to resolve interference:
    - Interferer related information
        - Internal/External interferer
        - Interferer id (in case it is an internal interferer)
        - Interferer capabilities (frequency band, transmission capabilities, etc.)
    - Information related to the capabilities of the involved Terminals
        - Terminal maximum/minimum transmit power
        - Supported frequency bands (e.g. ISM 2.4 GHz, ISM 5 GHz, 900 MHz)
        - Transmission capabilities (e.g. single carrier, carrier aggregation, modulations, coding rates)
        - Supported RATs

Decisions arisen from interference handling mechanisms that may be required to be exchanged over different interfaces for remote enforcement are:

- Low level node configuration information (for each reconfigured node)
    - Transmit power level
    - Transmit time
    - New frequency band
    - New RAT type
    - New Coding rate/modulation scheme
    - Time reservation information
    - Involved terminals
- High level node configuration information (for each reconfigured node)
    - Maximal message generation rate

4.5 Monitoring and reconfiguration/termination

The monitoring functionality is in charge of supervising the operation of the ON from its establishment until the ON is terminated. This functionality will dynamically acquire all the relevant information that may influence decision making processes around the life-time of the ON.

The monitoring functionality could trigger reconfiguration functionality that ultimately will decide on all the appropriate changes at the ON configuration. Reconfiguration decisions will be built upon node, route and spectrum identification and selection functionalities. Information exchange within the monitoring phase should enable to support the following reconfiguration triggers (the list is not exhaustive):

From ON-node perspective:

- New node(s) wishing to join an existing ON (& subsequent routing updates)
- Existing node(s) leaving ON coverage (& subsequent re-routing)
- Degradation in negotiated QoS parameters
- Changes in application QoS requirements.
- Spectrum/radio resource unavailability (node-initiated spectrum mobility/vertical HO)
- Changes in “user preferences” and/or terminal context
- remaining battery lifetime, changes in radio/link level parameters (SINR, BER, PER, etc.), propagation environment & mobility profile changes

From Network/infrastructure side:

- Need for load-balancing/congestion control across multiple ONs supported by a single infrastructure node
- Routing optimisation
- Degradation/improvements in negotiated QoS parameters
- Spectrum/radio resource availability (network-initiated spectrum mobility/vertical HO)
- Need to merge/split ONs/re-assign nodes
- Load-balancing across RATs
- Changes in network context information
- Potential for improvements in spectrum utilization
- Need for traffic offloading (via alternative RATs)

Note that whilst each ON node has only a local view of resource utilization and impact, the network node i.e. infrastructure part of ON, will have more of a global view and as such will attempt to optimise configuration settings of individual or groups of ONs under its control, in order to achieve better service quality and resource utilization.

As indicated above, the ON reconfiguration can be network-initiated or ON-node initiated. Reconfigurations can involve a single node, multiple nodes or the whole ON. The implementation of a reconfiguration decision would be mainly supported through ON Modification and, optionally, ON negotiation procedures (both addressed in section 5.3).

The monitoring functionality can also trigger the ON termination. Information exchange during for ON termination is related to the release of assigned resources and provision of

statistics (e.g., collected ON charging data), and in some cases, preparation of a handover to infrastructure. In particular, the following information is identified:

- Information related to the termination triggers:
    - Reason of termination (e.g. cessation of an application, lack of resources, poor QoS, high ON overhead)
    - Time to termination
    - Application identifier (necessary in case more than one application is supported by an ON)
- Information related to the handover to infrastructure
    - Information related to the application
        - Application type (e.g. real-time, interactive)
        - Bit rate required for the application
        - Application characterization (e.g. expected duration, elasticity, etc.)
    - Information related to the radio interface (for each active RAT and for each detected network access)
        - Measured Propagation loss
        - Measured Received Signal power
        - Measured Signal quality (e.g. SINR)
    - An indicator if a user can conduct a handover to infrastructure
    - Information about a new point of attachment
        - RAT type
        - Frequency band
    - Geographical location
    - Mobility level
- Information related to the resource release:
    - For each spectrum block forming the selected spectrum pool
        - Central frequency
        - Bandwidth
    - For gateway nodes
        - QoS currently provided (resources assigned)
        - QoS needed (resources needed)

4.6 Security and trust

The Security and Trust requirements for ON management are still under work. It is foreseen that "native" security obtained through RAT/CN-specific procedures will provide the basis for the complete Security framework. As additional procedures are likely to be needed, they

may be, either based on existing 3GPP mechanisms, or built as an additional Public Key-based scheme as described hereafter.

Security and trust functionality is intended to enable trust establishment and signalling data encryption between different heterogeneous devices. The functionality is needed during all ON phases and should prevent attacks conducted by outside nodes as well as inside nodes (some of the inside nodes could be compromised or could act selfishly).

Information exchange for Security and Trust is mainly related to the provision of digital credentials, public keys and access control policies. The digital credentials are related to various properties of a node and are used to establish a trust relationship between nodes without revealing their identities (each credential can be verified using the public key of a trusted third party). Access control policies govern access to specific services provided by a node (e.g. traffic relaying) and specifies credentials which needs to be submitted in order to gain access to those services. Public keys allows for the encryption of the signalling data.

In order to address the problem of internal attacks, the key revocation and key renewal mechanisms are needed. Implementation of such mechanisms requires exchange of information related to node accusations (generated by some missbehaviour detection mechanisms) between ON participants (each node is able to accuse other nodes of a malicious behaviour). Moreover, lists of revoked public keys need to be also exchanged.

Additionally, some information related to node capabilities with respect to security and trust could be exchanged. This information could include types of security mechanisms supported by a node and could be used to check whether a requested (by application) level of security can be provided by a node before the ON creation.

5. Control Channels for Coordination of Cognitive Management Systems (C4MS)

The following section provides a detailed description of the C4MS proposal. It introduces the common framework for enabling the exchange of signalling, context and policy information in heterogeneous environments and identifies potential C4MS implementation options.

5.1 Common framework

The following subsection introduces a common framework for the integration of CPC, CCR and CCC concepts introduced in Annex A Sections A.1, A.2, A.3, respectively. The framework is intended to allow the exchange of signalling, context and policy information between different network elements which may reside on the terminal side or on the infrastructure side. In the case that different protocols are used the transport of C4MS data, the framework shall also enable the interconnection/ interoperation between these different protocols. In order to enable that, the framework defines a basic set of common services, service access points, procedures (operations) and messages which should be supported by the C4MS (see Section 5.2 and 5.3). The framework is designed to allow the C4MS to meet the requirements (see Section 2) and enable the realization of the identified OneFIT scenarios.

Figure 5: C4MS framework – general view

In overall, the C4MS can be seen as an intermediate layer between C4MS users and the network protocol stack (see Figure 5) whose main role is to enable and coordinate the exchange of information between C4MS users located in different nodes. The C4MS may define and support several protocols to enable the information exchange between C4MS users. The protocols define message formats (including a message header and message parameters) and are envisioned to provide sufficient flexibility to enable C4MS information to be transported over different transport mechanisms (e.g. 3GPP RRC, OMA DM, IEEE MIH protocol), over different layers (L2, L3 and above). The C4MS messages, for example, can be transported over IP in order to be radio access technology independent or directly over MAC or RRC [12] messages in order to enable discovery procedures or communication before an IP connection is established.

The C4MS user is defined as a functional entity which uses the services provided by the C4MS in order to exchange the information with other C4MS users located in remote nodes. In order to access services provided by the C4MS, the C4MS user is required to register within its local C4MS entity. The two main users considered for the C4MS are CMON and CSCI; however, other functions like JRRM can also make use of the C4MS.In order to enable the proper operation the C4MS users shall be capable of:

- Transmitting and receiving information over SAPs
- Determination (and indication to the lower layers) of the transportation mechanism to be used (e.g. RRC, MIH, DIAMETER),
- Establishment and maintenance of multicast groups to enable transmission to multiple destinations (e.g. ON participants) at once
- Establishment and maintenance of routing tables

5.2 C4MS services and service access points

In order to enable the exchange of information between different C4MS users, six basic services have been identified as necessary:

- Information delivery
- C4MS discovery
- Addressing/Address mapping
- Security
- Message forwarding/relaying/proxying
- Message translation

Depending on the underlying transport mechanism, services related to acknowledgements, flow control, congestion control and message fragmentation/reassembly may also be required (e.g. in case that available transport protocols are not able to provide them).

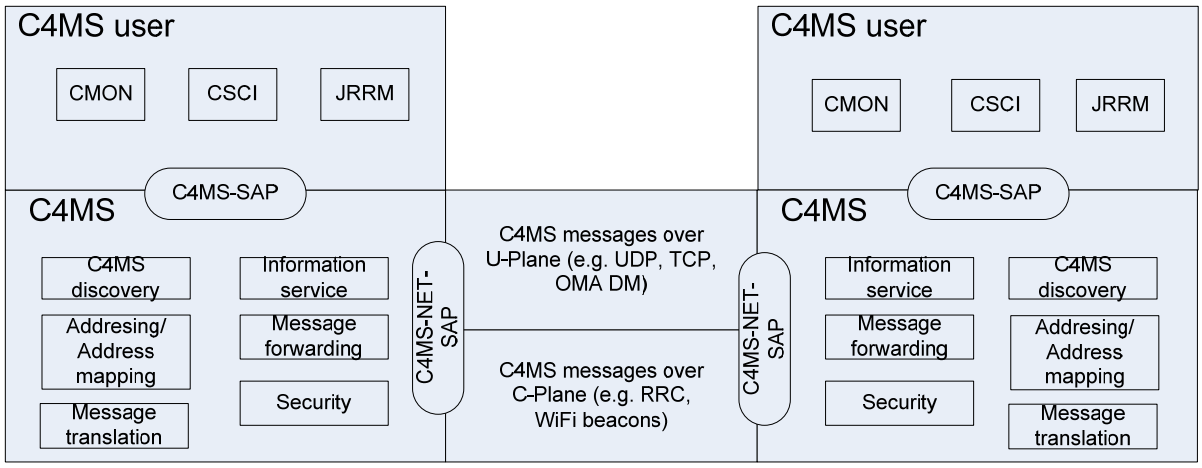


Figure 6: C4MS reference model

The C4MS services have the following functionality:

Information delivery: encompasses mechanisms for the information exchange between C4MS users. It supports information pull and push modes (requests/response and notification). It allows different types of information to be exchanged (e.g. commands, events or decisions). It allows for the delivery of information in a unicast, multicast and broadcast manner.

C4MS discovery: enables discovering of other C4MS users (on the terminal and network side) in case the necessary information is not provided by the lower layers (e.g. no extra information enabling discovery transmitted over beacons).

Addressing/Address mapping: enables the determination of the correct lower layer address of the remote C4MS user within the node (e.g. IP address and port number). This mechanism is necessary as different underlying layers can be employed for the transmission of C4MS data. The mechanism maintains a list of addresses of remote C4MS users (along with their lower layer addresses).

Security: provides means for establishing a secure connection between C4MS users belonging to the same ON. It supports mechanisms for encrypting and authenticating the exchanged messages as well as establishing a mutual authentication along with cryptographic key negotiation between C4MS users.

Message forwarding/relaying/proxying: enables exchange of messages between C4MS users which are not directly connected (in case necessary mechanisms are not provided by the underlying layers). The service is based on routing-related information carried by messages and routing table entries.

Message translation: enables translation between different C4MS protocols (different protocols may use different message formats and headers) thus allowing for the concurrent operation of different C4MS implementations which could be based on various transportation mechanisms. The service is especially necessary in case of heterogeneous scenarios in which different RAT dependent C4MS solutions could be deployed.

In order to enable to information exchange between C4MS users, two distinct Service Access Points (SAPs) were identifiedC4MS_SAP and C4MS_NET_SAP (see Figure 6).

C4MS_SAP: This media independent SAP provides a uniform interface to the C4MS users to use the services provided by the C4MS. Among others, the C4MS_SAP should support generic mechanisms for the messages to be sent and received.

C4MS_NET_SAP: This media dependent SAP provides transport services over the data/control plane of the underlying layers, supporting the exchange of C4MS information and messages with the remote C4MS users.

5.3 C4MS elementary procedures and messages

This subsection describes the first version of elementary ON management procedures and messages to be supported over C4MS. The following messages are currently proposed as an initial set for the interaction between CSCI/CMON entities which are C4MS users (the list was derived based on the Message Sequence Charts described in on D2.2 [3]):

- Information.Request, Information.Answer

- Discovery.Request, Discovery.Answer
- ON_Suitability.Indication
- ON_Negotiation.Request, ON_Negotiation.Answer
- ON_Creation.Request, ON_Creation.Answer
- ON_Modification.Request, ON_Modification.Answer
- ON_Release.Request, ON_Release.Answer
- ON_Status.Notification

The Messages are specified in this section using the ABNF specification. For more details on the ABNF specification, see IETF RFC 3588 [28], Section 3.2. As a short summary, the following syntax is used to define fixed, required and optional parameters (The parameters are called “AVPs”: Attribute-Value-Pairs as in [28]):

```
   message = header  [ *fixed] [ *required] [ *optional][ *fixed]

   fixed       = [qual] "<" avp-spec ">"
                 ; Defines the fixed position of an AVP

   required    = [qual] "{" avp-spec "}"
                 ; The AVP MUST be present and can appear
                 ; anywhere in the message (mandatory parameter)

   optional    = [qual] "[" avp-name "]"
                 ; The avp-name in the 'optional' rule cannot
                 ; evaluate to any AVP Name which is included
                 ; in a fixed or required rule.  The AVP can
                 ; appear anywhere in the message.

qual        = [min] "*" [max]
                 ; See ABNF conventions, RFC 2234 Section 6.6.
                 ; The absence of any qualifiers depends on whether
                 ; it precedes a fixed, required, or optional rule.
                 ; If a fixed or required rule has no qualifier,
                 ; then exactly one such AVP MUST be present.
                 ; If an optional rule has no qualifier,
                 ; then 0 or 1 such AVP may be present.
                 ;
                 ; NOTE:  "[" and "]" have a different meaning than in ABNF
                 ; (see the optional rule, above).
                 ; These braces cannot be used to express optional fixed
                 ; rules (such as an optional ICV at the end).
                 ; To do this, the convention is '0*1fixed'.
```

5.3.1 Information provisioning

The information provisioning procedure is used to exchange information between nodes.

Some examples where this procedure can be used are:

- retrieval of context information needed e.g. for the ON suitability determination
- retrieval of information on which spectrum to use for an ON

- exchange of information for the coordination of different networks

An example scenario is shown below:

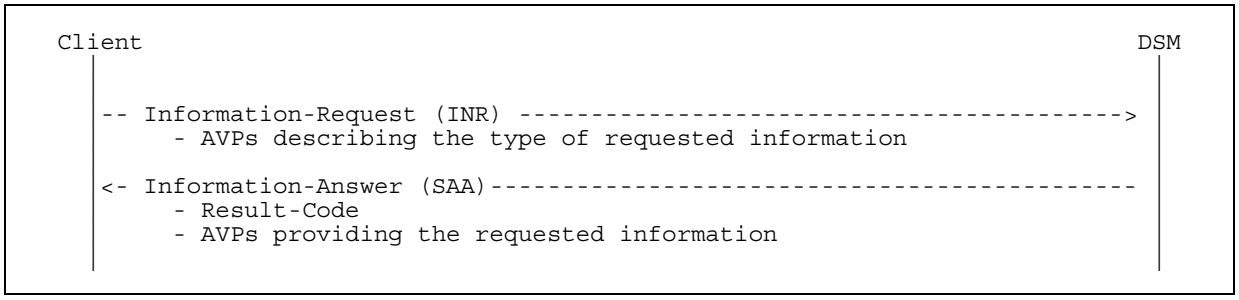


Figure 7: Information provisioning scenario

5.3.1.1 Information-Request (INR)

The Information-Request (INR) may be sent by any node to retrieve information from another node.

Message Format:

```
<INR> ::= <Header>
             * [ AVP ]
```

5.3.1.2 Information-Answer (INA)

The Information-Answer (INA) is sent in response to the INR to provide the requested information or to indicate why this was not possible.

Message Format:

```
<INA> ::= <Header>
               { Result-Code }
             * [ AVP ]
               [ Error-Message ]
             * [ Failed-AVP ]
```

5.3.2 ON Suitability

The ON Suitability procedure is used by a first node to initiate the ON suitability determination in a second node (see Figure 8).

This procedure is typically used in scenarios where the Node 1 has discovered a situation where an ON consisting of other nodes may be suitable, but where Node 1 is not necessarily part of the ON and thus cannot decide on the suitability of an ON. Examples for such scenarios are the opportunistic capacity extension scenario (Scenario 2 in D2.2 [3]) or the infrastructure created opportunistic ad-hoc networking (Scenario 3 in D2.2).

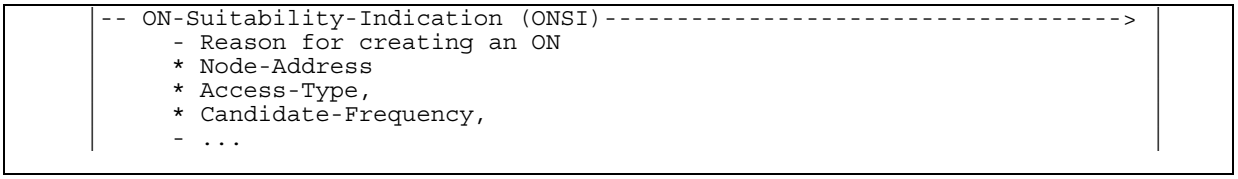


Figure 8: ON Suitability Procedure

5.3.2.1 ON-Suitability-Indication (ONSI)

The ON-Suitability-Indication (ONSI) shown in Figure 8is sent by a node to initiate the ON suitability determination in another node.

Message Format:

```
<ONSI> ::= <Header>
                { Reason  }
              * { Node-Address }
              * [ Access-Type ]
              * [ Candidate-Frequency ]
              * [ AVP ]
```

Parameters:

- Reason: The reason for creating an ON e.g. low QoS or load of the surrounding BSs
- Node-Address(es): List of nodes potentially involved in an ON
- Access-Type: RAT(s) proposed for the ON. This information may be used to switch on those RATs for the discovery procedure.
- Candidate-Frequency: Allocated or candidate spectrum band(s),
- Other parameters (FFS)

5.3.3 Node discovery

The node discovery procedure is used by a first node to discover other nodes in its vicinity. Such procedures typically exist in each RAT.
For opportunistic networking, the existing node discovery procedures should be extended to indicate if a node is supporting opportunistic networking (e.g. by adding extra parameters). Then the node discovery procedure can also be used to detect ON-capable nodes.
In existing RATs, two types of procedures can typically be used:

5.3.3.1 Listen on broadcasted information (Beacons/Broadcast channel information)

A node 1 (e.g. a terminal) listens on broadcasted information sent out by another node (e.g. a base station, a WLAN Access Point or a terminal in an ad-hoc network) as illustrated in Figure 9.

Existing broadcast information may be extended to provide additional information if opportunistic networking is supported. If such information cannot be provided in a beacon, this information must be retrieved via other procedures.

Dependent on the radio access technology, different methods are used to broadcast information:

- Beacons are used e.g. in 802.11 WiFi networks [14]to periodically send out information like Service Set Identifier (SSID), timestamp, supported data rates and capability information. Beacons are sent out by access points as well as typically by at least one node in an ad-hoc network.
- Broadcast messages are used by base stations (e.g. GSM, UMTS, LTE) to provide cell-related information to all users in a cell.

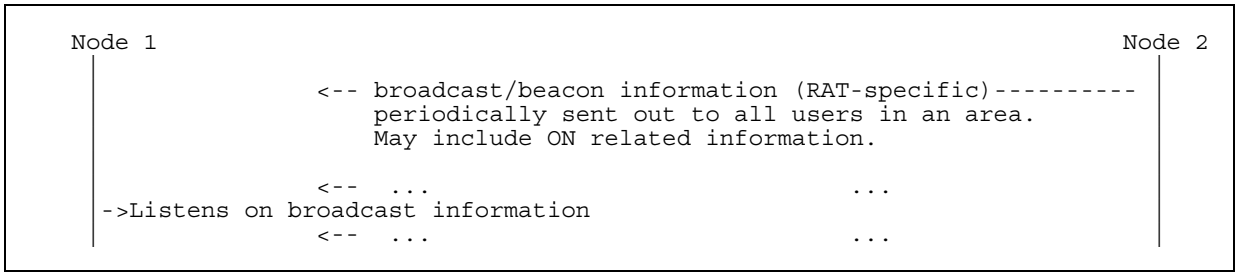


Figure 9: Broadcast based ON Discovery Procedure

5.3.3.2 Request/Response based discovery (e.g. probing)

A node 1 (e.g. a terminal) sends out a discovery-request (e.g. probe-request in 802.11) and waits for a discovery-answer (e.g. probe-response in 802.11) as shown in Figure 10. Such a discovery response contains information like capability information and supported data rates. As an extension for opportunistic network, additional information may be added to indicate if opportunistic networking is supported, e.g. by extending 802.11u [15]. If such information cannot be provided in the discovery-answer/probe-response, this information must be retrieved via other procedures.

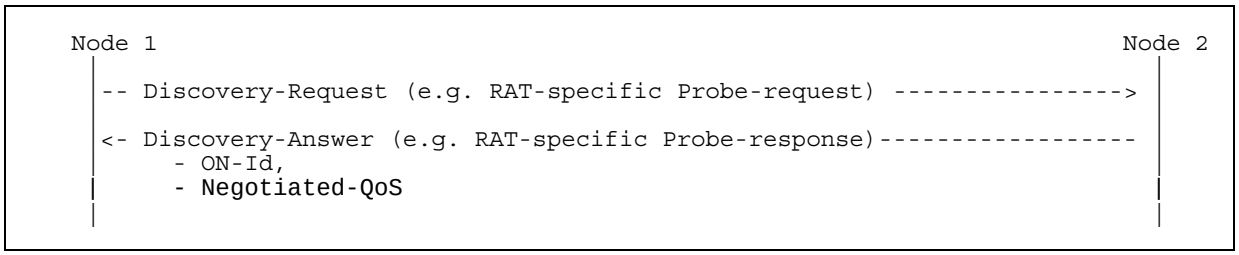
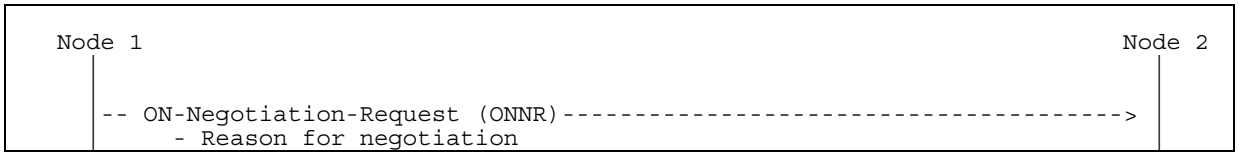


Figure 10: Request/response based discovery procedure

5.3.4 ON Negotiation

The ON Negotiation procedure is used to negotiate about the creation or modification of an ON, e.g. if a node is willing to join an ON, the conditions for joining and to exchange node capabilities and context information.

An example ON Negotiation is shown in Figure 11 below:



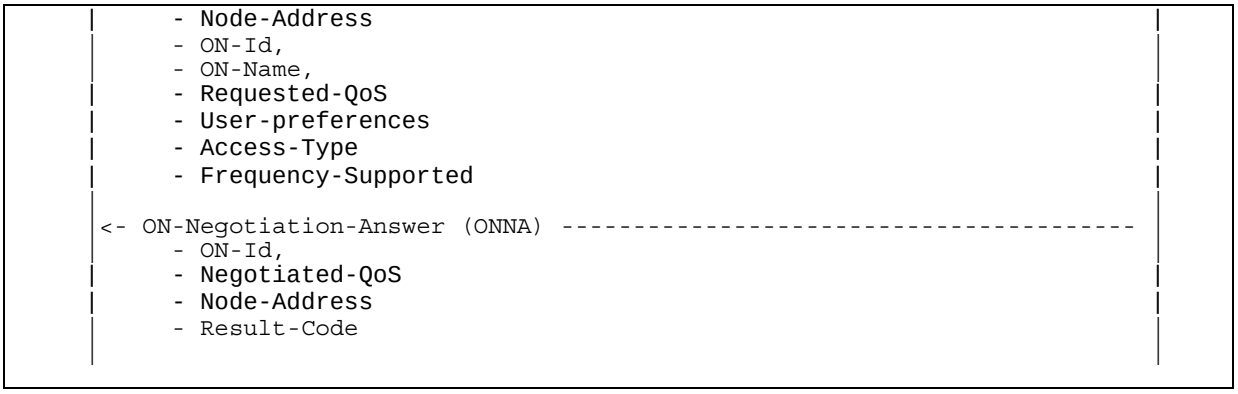


Figure 11: ON Negotiation Procedure

5.3.4.1 ON-Negotiation-Request (ONNR)

The ON-Negotiation-Request (ONNR) may be sent by any node to negotiate about the creation or participation in an opportunistic network.

Message Format:

```
<ONNR> ::= <Header>
                { Reason }
              * { Node-Address }
                { ON-Id }
                { ON-Name }
                [ Requested-QoS ]
                [ User-preferences ]
              * [ Access-Type ]
              * [ Frequency-Supported ]
              * [ AVP ]
```

The Node-Address may include further info, e.g. if it is a source node or a relay node.

The message contains information on capabilities (e.g. supported RATs and frequency bands, maximum transmit power) and requirements (e.g. QoS, latency, bit rate) of nodes.

5.3.4.2 ON-Negotiation-Answer (ONNA)

The ON-Negotiation-Answer (ONNA) is sent in response to the ONNR. The ONNR includes if a node is willing to participate in an ON.

Message Format:

```
<ONNA> ::= <Header>
              { Result-Code }
            * { ON-Id }
            * { Node-Address }
              [ Negotiated-QoS ]
              [ Error-Message ]
            * [ Failed-AVP ]
            * [ AVP ]
```

5.3.5 ON Creation

The ON Creation procedure is used to create an ON after successful negotiation.

An example scenario is shown in Figure 12below:

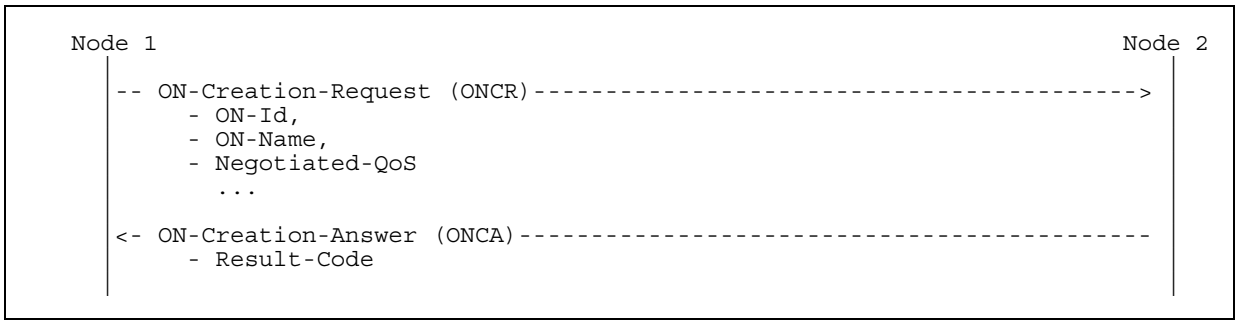


Figure 12: ON Creation Procedure

5.3.5.1 ON-Creation-Request (ONCR)

The ON-Creation-Request (ONCR) is sent to create an Opportunistic Network. This message can contain the detailed information of the ON such as the nodes involved and the spectrum band to be used.

Message Format:

```
<ONCR> ::= <Header>
                { ON-Id }
                { ON-Name }
              * { Node-Address }
                [ Negotiated-QoS ]
                [ Geographical-Location ]
              * [ AVP ]
```

5.3.5.2 ON-Creation-Answer (ONCA)

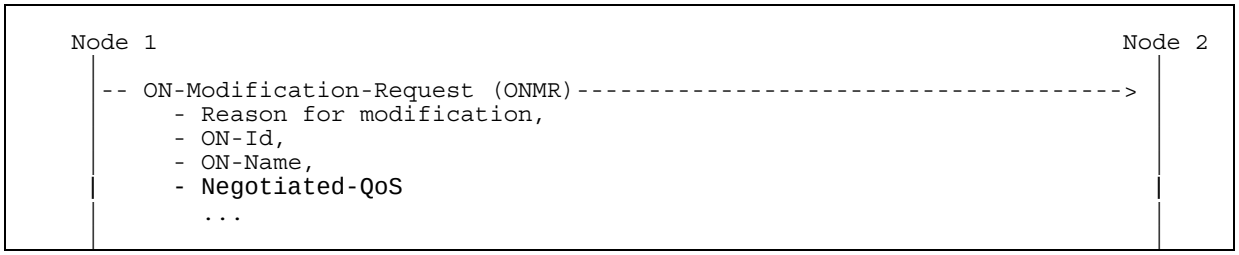
The ON-Creation-Answer (ONCA) is sent in response to the ONCR and indicates if the ON is successfully created or not.

Message Format:

```
<ONCA> ::= <Header>
                { Result-Code }
                [ Error-Message ]
              * [ Failed-AVP ]
```

5.3.6 ON Modification

The following procedure illustrated in Figure13is used to enable a modification of an ON configuration. The modification can be conducted for a single node, multiple nodes or the whole ON. A negotiation procedure may be optionally executed before the ON Modification is executed.



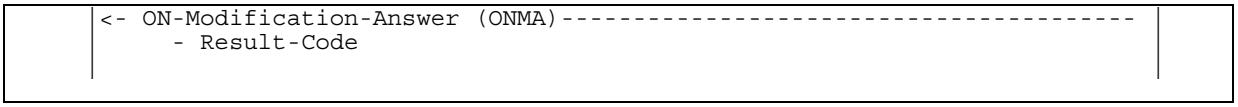


Figure13: ON Modification Procedure

5.3.6.1 ON-Modification-Request (ONMR)

The ON-Modification-Request (ONMR) may be sent by any node to modify the configuration of an opportunistic network.

Message Format:

```
<ONMR> ::= <Header>
                { Reason }
                { ON-Id }
                { ON-Name }
              * { Node-Address }
                [ Negotiated-QoS ]
              * [ AVP ]
```

5.3.6.2 ON-Modification-Answer (ONMA)

The ON-Modification-Answer (ONMA) is sent in response to the ONMR and indicates if the ON is successfully modified or not.

Message Format:

```
<ONMA> ::= <Header>
                { Result-Code }
                [ Error-Message ]
              * [ Failed-AVP ]
```

5.3.7 ON Release

The ON Release procedure is used to release a node from the ON or to release the complete ON. An example scenario is shown in Figure 14 below:

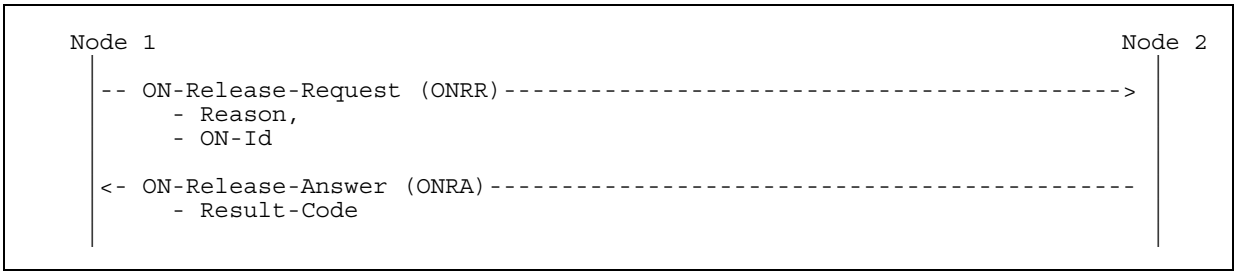


Figure 14: ON Release Procedure

5.3.7.1 ON-Release-Request (ONRR)

The ON-Release-Request (ONRR) is sent to release a link or a node from an ON.

Message Format:

```
<ONRR> ::= <Header>
                { Reason }
                { ON-Id }
              * [ AVP ]
```

5.3.7.2 ON-Release-Answer (ONRA)

The ON-Release-Answer (ONRA) is sent in response to the ONRR.

Message Format:

```
<ONRA> ::= <Header>
                { Result-Code }
[ Error-Message ]
              * [ Failed-AVP ]
```

5.3.8 ON Status Notification

The procedure is used by a first node to inform a second node about the status or status changes in an ON. A Notification-Event-Type describes the event to be reported, e.g.

- ON_Negotiated
- ON_Created
- ON_Modified
- ON_Released

This procedure is used for example to notify the infrastructure about creation, modification or release of an ON and may be used e.g. for accounting and billing purposes.

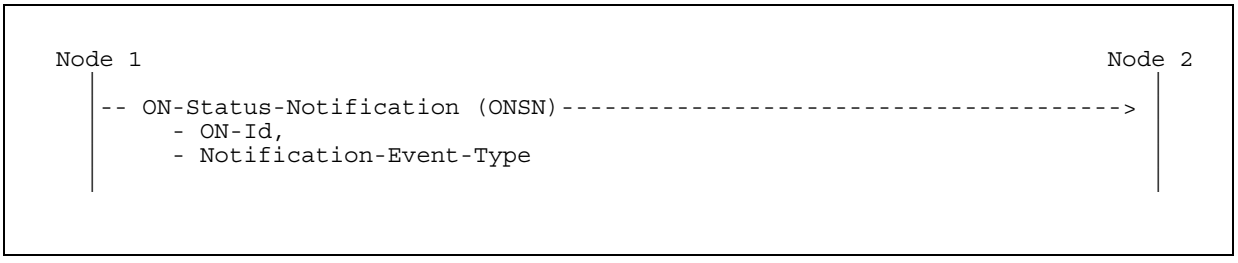


Figure 15: ON Status Notification Procedure

5.3.8.1 ON-Status-Notification (ONSN)

The ON-Status-Notification (ONSN) may be sent by any node to notify about a status of an ON.

Message Format:

```
<ONSA> ::= <Header>
                { ON-Id }
                { Notification-Event-Type }
              * [ AVP ]
```

Further information like involved nodes, type of applications, time and amount of exchanged data can be included in this message.

5.3.9 Security related procedures

5.3.9.1 Transmission level security

It shall be possible to transport the C4MS messages in a secured way. Dependent on the chosen approach (see section 5), this can be made via RAT-specific security procedures or via higher layer procedures like IPsec [26] or TLS [25].

5.3.9.2 Authentication and Authorization

In order to provide Authentication and Authorization, existing security mechanisms shall be reused. Dependent on the chosen approach (see sections5.4 and 5.5), this can be made via RAT-specific security procedures or via higher layer procedures.

Security related parameters may be included in the previously described messages or may be exchanged using additional messages.

One example of a higher-layer Authentication and Authorization procedure using additional messages is the Re-Auth-Request/Response as defined in the Diameter base protocol [28]:

The Re-Auth-Request (RAR), may be sent by any server to the access device that is providing session service, to request that the user be re-authenticated and/or re-authorized.

Message Format:

```
<RAR>  ::= < Header >
< Session-Id >
                  { Origin-Host }
                  { Origin-Realm }
                  { Destination-Realm }
                  { Destination-Host }
                  { Auth-Application-Id }
                  { Re-Auth-Request-Type }
                  [ User-Name ]
                  [ Origin-State-Id ]
                * [ Proxy-Info ]
                * [ Route-Record ]
                * [ AVP ]
```

The Re-Auth-Answer (RAA) is sent in response to the RAR. The Result-Code AVP MUST be present, and indicates the disposition of the request. A successful RAA message MUST be followed by an application-specific authentication and/or authorization message.

Message Format:

```
<RAA>  ::= <Header>
< Session-Id >
```

```
   { Result-Code }
   { Origin-Host }
   { Origin-Realm }
   [ User-Name ]
   [ Origin-State-Id ]
   [ Error-Message ]
   [ Error-Reporting-Host ]
 * [ Failed-AVP ]
 * [ Redirect-Host ]
   [ Redirect-Host-Usage ]
   [ Redirect-Host-Cache-Time ]
 * [ Proxy-Info ]
 * [ AVP ]
```

5.4 RAT/System Independent implementation options

The following section provides descriptions of several possible C4MS implementation options which are independent from the underlaying transportation mechanisms. The following table shows the overall pros and cons of the RAT/System independent solutions.

Pros	Cons
• Independent of the underlying System/RAT (no modification of underlying RATs required) • Support for multihop scenarios (most cases)	• Requires connection establishment for the information exchange (high delay and additional overhead) • High protocol overhead • Contention with the user data (high delay)

Table 2: Advantages and Disadvantages of a RAT independent approach

5.4.1 IETF DIAMETER based approach

The DIAMETER base protocol is an extensible protocol originally designed to provide an Authentication, Authorization and Accounting (AAA) framework for applications such as network access or IP mobility. Diameter is also used in 3GPP based networks to access the Home Subscriber Server (HSS) [9]. For more details, see also Appendix A.10.

The advantages of the Diameter protocol as defined in IETF RFC 3588 [28] is that

- it is an easily extensible protocol to which new building blocks can be added for different applications;
- it provides already security framework including Authentication, Authorization and Accounting (AAA); User authentication information is transported for the purpose of enabling the Diameter server to authenticate the user.
- relaying of messages is supported: Diameter relays forward requests and responses based on routing-related AVPs and realm routing table entries. Since Diameter relays do not make policy decisions, they do not examine or alter non-routing AVPs.
- proxying of messages is supported: In addition to forwarding requests and responses, Diameter proxies make policy decisions relating to resource usage and provisioning.

- proxying is supported: Messages can be sent over different hops and each node may make necessary updates.
- Diameter is a well established protocol used e.g. also in 3GPP [9]

Diameter is thus a candidate protocol for the C4MS as C4MS messages and paramters can be defined as extensions to the Diameter base protocol.

Some existing Diameter messages may also be used for the maangement of opportunistic network. While the ON-Release-Request/Answer is defined in section 5.3.7, the Diameter Disconnect-Peer-Request/ Answer messages may be used in certain cases to disconnect the transport layer of a peer. Instead of the ON_Status_Notification messages as defined in section 5.3.8.1 the Diameter Accounting-Request/Answer may be used to inform the infrastruture about the creation or release of an ON. Further on, the Capabilities Exchange messages should be used to allow the discovery of a peer's identity and its Diameter capabilities (protocol version number, supported Diameter applications, security mechanisms, etc.)

Like the other options using IP transport, this option can only be used if an IP connection is already available but not in phases like discovery.

5.4.2 IEEE 802.21 MIH based approach

The IEEE 802.21 "Media-Independent Handover (MIH) Services" standard [15] provides a set of extensible mechanisms targeted to enable the optimization of handovers between heterogeneous IEEE 802 systems as well as facilitate handovers between IEEE 802 systems and cellular systems (e.g., 3GPP and 3GPP2). The main features of the standard have been summarised in appendix A.7. Over such a basis, this section discusses the suitability of IEEE 802.21 standard to support the functionalities and procedures envisioned for C4MS protocols. In particular, potential extensions of the standard to address policy and context information transfer, operational control and management procedures and distributed communications models are addressed.

Extensions for context information transfer

The Media Independent Information Service (MIIS) is built on the specification of various Information Elements (IEs) that can be transferred between remote MIHF entities. The list of IE's specified so far in the standard basically covers: (1) general and access network specific information, (2) point of attachment (PoA) specific information and (3) other information that is access network specific, service specific, vendor/network specific. While some of these IE's can be useful in the framework of C4MS, it is expected that further context awareness information needs to be distributed among different ON nodes (e.g., transfer of spectrum opportunities for secondary access). This could be accomplished by extending the set of IE's.

IEs can be represented by means of two distinct methods specified in the standard: Binary representation and Resource Description Framework (RDF) representation that is a general-purpose language for representing information in the Web [38]. In the former case, each IE is assigned a given binary identifier so that the addition of new IEs for other purposes than

handover optimization is possible but requires an extension of the standard. On the contrary, in the case of RDF representation, it is possible to define an extended schema to introduce new IEs without requiring further modifications to the standard. Hence, as far as the required cognitive context information can be specified by means of a RDF model, current MIIS service could be leveraged to distribute policy and context awareness information.

It is worth noting that the implementation of C4MS based on 802.21 would require all of the network entities, which support the OneFIT system, to support MIIS and employ local information server. Additionally, as MIIS is conceived to provide mobile terminals with details on the static characteristics and services of the serving and neighbouring networks (e.g., network type, operator identifier, frequency bands, etc.) some changes to the MIIS may be required.

Extensions for operational control and management procedures

In addition to context information transfer, C4MS shall support the necessary signalling required in the opportunistic network (i.e., the set of procedures to control and manage the ON operation). Whenever interactions between C4MS users and required signalling procedures can be built upon an interaction model based on the transfer of parameter-setting or parameter-extracting commands and the configuration and reporting of remote events, MICS and MIES can effectively constitute a valid implementation framework. To that end, the MIH standard should be extended by defining a new set of “commands” and “events” specifically targeted to achieve the operational control and management of the cognitive radio network. So far, current support for command and event services in MIH is specific for handover optimisation. In any case, though the extension of the MIH command/event model could be a plausible approach to manage interaction between C4MS users, at the current stage, C4MS is envisioned to support information exchange only between remote peer C4MS user entities. Under this view it is considered that a “generic” information delivery service is sufficient to support operational control and management procedures.

Extensions for distributed communications models

Communications models needed for C4MS in opportunistic networks may require both network to device communications but also device to device communications. In this regard, current MIHF communication model is mainly driven by handover optimisation and is focused on MIH information exchanges between a MIHF entity in the terminal and a set of MIHF entities within serving and neighbouring networks. Therefore, appropriate extensions may be needed to cover also signalling transfer between terminals. These extensions may encompass trusted relationship management between terminals in order to announce and/or grant access to supported MIH-like services as well as routing mechanisms of MIH signalling messages.

5.4.3 3GPP ANDSF/OMA DM based approach

Providing assistance information from the infrastructure is a key feature in OneFIT.

For the support of intersystem mobility in cases where multiple heterogeneous access radio access networks are available, 3GPP has specified the Access Network Discovery and Selection Function (ANDSF) [5]. The ANDSF provides information about available networks (3GPP as well as non-3GPP access networks). The ANDSF framework which uses

This ANDSF framework using the OMA Device Management (see Appendix A.4 and A.5) may also be part of the C4MS solution, especially to provide context information about availablen access networks from the infrastructure to the users.solution. However, it has to be noted that this option is only useful for the communication between a terminal and the infrastructuire but is typically not used for the communication between different terminals.

Since the ANDSF is operator-controlled, it is typically used for distributing information related to access networks being under the control of the operator owning the ANDSF. While it is in theory possible to extend the ANDSF MO to Cognitive Radio related parameters, it is of limited usefulness in a multi-operator heterogeneous environment and should thus be tailored to the needs of a single operator.

Further, it has to be noted that the ANDSF communication mechanisms are not used for the communication between different terminals.

5.4.4 Distributed Agents' based approach

This section outlines aspects of the implementation of C4MS with the use of a multi-agent environment. Within such a multi-agent environment/system, every component (such as a network infrastructure element, a user device or management software) can be represented by one or more intelligent agents that act as a mediator between the components' functionality and the rest of the system. Thus, each system component is loosely coupled to other components and can interact by exchanging messages through a high level interface. In such a context, C4MS can be seen as a RAT-agnostic, upper layer logical communication channel (mainly over TCP/IP) between distributed agents/agent platforms residing in both terminal and network sides and used for the conveyance of context information. The corresponding information flow can be formulated as an ontology that can be easily extended or modified.

The work of Foundation for Intelligent Physical Agents (FIPA) [46], which is an international non-profit association of companies and organizations with the aim of generating specifications of generic agent technologies, can be used to provide a standardized, transport solution for such C4MS communication. More specifically, in order to promote interoperability between agent platforms, a number of standard MTPs (Message Transport Protocols) and MTP interfaces have been defined by FIPA, in particular an MTP based on the Internet Inter-Object request broker Protocol (IIOP) defined by OMG. In addition, FIPA neither defines nor requires a specific protocol for intra-platform message delivery and each implementation can choose any Internal Message Transport Protocol (IMTP).

Framed within the above, JADE [47] (JADEX [48]) is a robust, fully Java and FIPA compliant framework for developing distributed agent systems and can run on both PCs and wireless devices that support Java Micro Edition (Java ME) using the package developed by the Lightweight Extensible Agent Platform (Leap) Project. JADE components exchange messages which are serialized and transmitted over TCP, according to the FIPA Agent Communication Language (ACL) message structure specification.

The JADE messaging architecture differentiates between intra-platform and inter-platform communication. In the case of intra-platform communication, agents reside in the same platform and JADE uses its IMTPs for implementing delivery services. In order to minimize delivery time, JADE selects the most appropriate transport mechanism further distinguishing between the case of communicating agents that reside in the same container and agents that reside in different containers. A container, which is hosted by a Java Virtual Machine, provides the run-time environment and the services for one or more agents. More specifically, for the case of intra-platform communication, JADE utilizes:

- Event passing when both the sender and receiver agents are in the same container.
- Remote Method Invocation (RMI) when the sender and receiver agents are in different containers.

In the case of inter-platform communication, the following MTPs are currently available for interaction among agents:

- CORBA IIOP MTP based on standard Sun ORB provided with the JDK (the default installation).
- CORBA IIOP MTP based on ORBACUS [49].
- HTTP-based MTP.

Information on relevant implementations of the CPC concept are provided in A.9.

5.4.5 Network management system based approach

The following section reviews a possible option for the implementation of C4MS based on network management systems. The basic idea of this approach is to use mechanisms and protocols employed by O&M systems and extend it to enable the exchange of ON relevant data (i.e. ON management signalling and ON relevant context information) between different network elements.

As mentioned, the application of O&M systems for the exchange of C4MS data requires certain extensions. On the side of Configuration Management (CM) a major leap is required to move away from human-controlled model of applying CM changes towards automation-controlled model. Within C4MS domain CM changes need to be applied immediately and any delay, usual in today's human-controlled systems (single minutes to hours), would almost certainly invalidate decision resulting from the delivered data.

In case of the Performance Management (PM) a new approach for measurement data collection is needed (current PM data collection methods are too slow). The new approach should allow that for certain PM data (relevant for Opportunistic Networks) triggers are defined that raise C4MS-related alarms which are passed to the network management system.

Fault Management (FM) needs to define a new set of ON specific alarms which would be generated whenever ON relevant data needs to be reported. The alarms in the C4MS framework would provide a complementary function to the PM triggers.

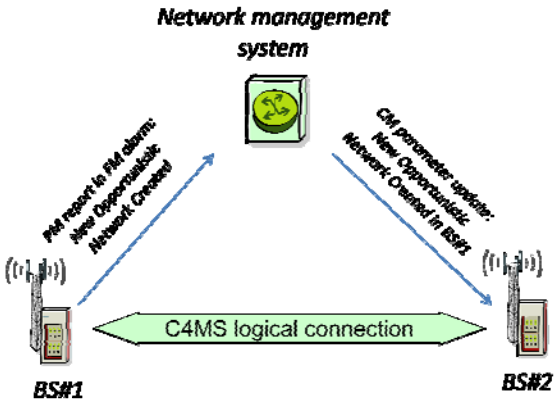


Figure 16: O&M based approach - general view

As O&M systems have not been designed to enable the exchange of information between manageable network elements, the C4MS layer located in the network management system side is required to forward C4MS messages from one network element to another. The C4MS message forwarding service requires C4MS layer to be capable of translating C4MS messages which are received in a form of PM reports carried by FM alarms into C4MS messages carried in a form of simple CM procedures such as "update value" (e.g. CM procedures could create a new manageable object which holds information related to the ON created in the neighbouring Base Station).

On the network element side the C4MS layer would be responsible for generation and reception of C4MS messages. The generation of C4MS messages could be achieved by translating C4MS messages into simple procedures related to setting certain objects/parameters monitored by the management agents. The reception of C4MS messages would require a simple object/parameter reading.

Network management system based approach	
Pros:	Cons:
• No direct signalling between GERAN, UTRAN, E-UTRAN and non-3GPP access networks • Minimal impact on the existing GERAN, UTRAN, E-UTRAN protocols • No additional Iur, Iurh, Iur-g , X2, Iu, and S1 load generated • Possibility to support C4MS in legacy systems	• Additional load of network management systems (e.g. R, B interfaces in 3G/4G NMS) • Extension of Performance Monitoring (PM) and Configuration Management (CM) interfaces • Integration and synchronization of different management systems

Table 3: Advantages and Disadvantages of a network management system based approach

5.4.5.1 TR-069

TR-069[36] as specified by the Broadband forum is one of the possible protocols which could be potentially used for the implementation of the C4MS based on the network management system approach described above. The protocol is widely used for the management of DSL devices and recently has been approved by 3GPP as a protocol suitable for the management of HNBs (see Appendix A.11). TR-069 already provides several methods which can be reused for the purpose of the ON management and context information exchange. The relevant methods are:

- Inform – allows CPE to "inform" ACS about parameter settings. One of the relevant arguments of this method is the list of parameters which can be used to carry the ON relevant data (the inform method can be initiated periodically or on parameter change, if Active Notification Attribute is set).
- GetParameterValues – allows ACS to get specific CPE parameter values. The parameter values in this case can be also treated as measurement results which could be continuously updated by C4MS users.
- SetParameterValues – allows ACS to update specific CPE parameter values which could be responsible for the ON management.
- Download – allows CPE to download files on ACS request. The method could be used to transfer ON relevant data stored in a file from ACS to CPE (e.g. new ON settings).
- Upload – allows CPE to upload files on ACS request. The method could be used to transfer ON relevant data stored in a file from CPE do ACS (e.g. measurement results).

C4MS data in this case could be transmitted either in a form of a list of parameters to update/read (some of the parameters could be considered as read-only values and could be used to present results of some measurements) or 2) in a form of information stored in a file which can be further uploaded or downloaded by the managed device.

5.4.5.2 Simple Network Management Protocol (SNMP)

SNMP could be another protocol potentially used for the implementation of the C4MS based on the network management system approach. SNMP is an IP based protocol used for managing and monitoring devices in an IP network [27]. Similarly to TR-069, SNMP also provides several methods which could be reused for the purpose of the ON management and context information exchange. The relevant methods include:

- Trap – allows agents to notify managers about significant events (e.g. changes in the parameter settings). In order to enable transmission of ON related data new vendor specific traps could be defined.
- GetRequest – allows manager to request from agent a set of parameter values. The requested parameters in this case could store different ON related information such as ON relevant measurement results or ON routing settings
- SetRequest – allows manager to set values of specific parameters in agents which could be responsible for the ON management (e.g. updating routes, spectrum reallocation).
- Response – used to return requested information from agent to manager. The message could carry information relevant to the ON management or ON context information.

5.5 RAT/System dependent implementation options

The following section provides descriptions of possible C4MS implementation options which are dedicated for specific transportation mechanisms. The following table shows the overall pros and cons of the RAT/System dependent solutions. The pros and cons of the individaual approaches are discoussed separetely in each subsection.

RAT dependent approach	
Pros	Cons
• No contention with the user data (low latency) • In most cases connection setup not required for the exchange of information (low overhead and latency) • Support for the efficient C4MS discovery	• Dependant on the underlying System/RAT (multiple solutions are required) • May require RRC/MAC alternation • Information exchange only for a single hop (multihop requires additional extensions)

Table 4: Advantages and Disadvantages of a RAT dependent approach

5.5.1 3GPP based approach

The following section reviews possible implementation options for the exchange of context information, policies and ON management signalling between entities within 3GPP networks based on the reuse of the existing 3GPP interfaces and protocols. The proposed options assume that CSCIs and CMONs reside within network entities which are part of a 3GPP system. The C4MS for the proposed implementation options could be seen as a new application (such as RIM application) which resides in the 3GPP terminal/network entity.

3GPP based approach	
Pros	Cons
• High reliability • Evolutionary approach – extension to already well defined standards • Repetitive transmission (other 802.11 IEs may not be required)	• Increased signalling over the infrastructure • Impact on the existing interfaces and protocols • Inter-operator signalling within 3GPP and signalling between 3GPP and non-3GPP access networks not possible, other means and interfaces must be devised (e.g. via additional entities not residing in RAN)

Table 5: Advantages and Disadvantages of a 3GPP based approach

5.5.1.1 3GPP Air Interface Aspects

As described in detail in Appendix A.13 in E-UTRAN, the System Information (SI) acquisition is possible in RRC IDLE and RRC CONNECTED states. For transport of C4MS related information in downlink that is relevant to all UEs in coverage extending the System Information (SI) broadcast methods of RRC seems to be a good idea. Such an extension would have to support exchange of general information about e.g.:

- available infrastructure elements for both 3GPP and no-3GPP infrastructure
- policy related to forming an ON (e.g. whether it is permitted, under what circumstances etc.)
- available spectral resources for ON formation (e.g. TV WS spectrum)

However, for other types of C4MS related information, such as distinct commands that are only relevant for a certain UE, e.g. to establish or release a connection, a dedicated signalling method is needed. For this some modifications to the Direct Information Transfer procedures of UMTS and LTE are envisaged. These extensions shall enable the transfer of C4MS PDUs over Iub (UMTS) and Uu (UMTS/LTE) air interfaces to selected peer entities (in contrast to the broadcast of data described above). The relevant procedures which require alteration are:

- RRC: UL Direct Information Transfer
- RRC: DL Direct Information Transfer

For example, in LTE the "dedicatedInfoType" IE that is used in the *DLInformationTransfer* and *ULInformationTransfer* RRC Messages could be enhanced. The enhancements could be achieved, for instance, by adding a parameter like "dedicatedInfoOneFIT" to create a new "channel" on top of RRC (non access stratum). If the "dedicatedInfoOneFIT" IE is used, OneFIT specific messages are exchanged and C4MS signalling is enabled between a UE and the infrastructure. This would however only work for distinct UEs that are residing in RRC_CONNECTED state. If a UE in RRC_IDLE was to send some C4MS data in UL direction, it would be required to kick-off the connection setup procedure (which consists of three transactions). The last of these messages is called "RRCConnectionSetupComplete" and would be used to indicate with the new "dedicatedInfoOneFIT" IE if C4MS data is conveyed (in piggybacking mode).

Regardless of the state an LTE UE is in: additional integrity protection and ciphering can be defined and applied at the "OneFIT layer" if we see a need for it.

5.5.1.2 3GPP Core Network Aspects

Radio Network Subsystem Application Part (RNSAP):

Assuming that the CMON and CSCI reside within the UTRAN/GERAN, the exchange of C4MS PDUs between network entities could be realized over the Iur, Iur-g or Iurh interfaces. It is worth noting that RNSAP protocol already provides several procedures which could be reused for the purpose of C4MS data provision. The relevant procedures are: Information Exchange and Direct Information Transfer [7]. The necessary RNSAP extensions could be achieved then by modifying message structures used for these procedures (adding the optional ON relevant information elements to carry C4MS PDUs).

It is worth noting that the existing RNSAP procedures already allow the exchange of different cellular network related context information (different measurement results, system information, etc.). The content of C4MS PDUs could be then limited only to the ON management signalling messages and context information related to non-3GPP access networks.

X2 Application Part (X2AP):

In case CMON and CSCI reside within E-UTRAN, the exchange of ON related information could be supported over the X2 interface. In order to enable the exchange of context and policy information as well as ON management signalling, X2AP protocol needs to be extended. Similarly to RNSAP, various existing X2AP procedures can be reused for this purpose (e.g. eNB Configuration Update). The message structures used for one of the existing procedures could be modified by adding new, optional ON relevant information

elements. The alternative here is to introduce a new procedure used solely for the purpose of the C4MS PDU exchange.

Similarly to RNSAP, X2AP protocol enables provision of different cellular network related context information which can be used for the purpose of ON management (e.g. load indication, Resource Status Reporting Indication, Resource Status reporting). The content of C4MS PDUs could be then also limited to the ON management messages and context information related to non-3GPP access networks.

Radio Access Network Application Part (RANAP) and S1 Application Part (S1AP):

The coordination of the infrastructure entities within 3GPP networks needs to be additionally realized over the Iu, Iuh and S1 interfaces. The employment of the interfaces is necessary in order to:

- enable inter-system exchange of information,
- enable the exchange of context and policy information between HNBs and RNCs ,
- support scenarios in which cognitive management entities reside within the CN.

In order to realize the necessary functionalities, RANAP and S1AP protocols need to be extended to support the provision of the C4MS PDUs. The extension could consider the Direct Information Transfer procedure. The procedure is used for the transfer of information between RAN and CN and enables exchange of different information (e.g. RAN Information Management (RIM)) between different 3GPP RANs. Both protocols could be extended by adding a new Inter-system Information Transfer Type (see [7] section 9.2.1.62 and [13] section 9.2.1.55). The new Inter-system Information Transfer Type should enable transfer of C4MS PDUs.

It is worth noting that RANAP and S1AP protocols do not support provision of cellular network related context information thus the content of C4MS PDUs must not be limited to the ON management messages and context information related to non-3GPP access networks.

It is worth noting that the above-mentioned placement of cognitive management entities supporting C4MS within CN (see the bullet point above) needs further study to elaborate pros and cons of such approach. It is anticipated that the volume of data related to exchange of information needed to form ON will be of similar order as in case of mobility management and resources management. Consequently, the processing capabilities required to handle ON-related information will put additional requirements on CN infrastructure yielding a substantial investment by MNOs. Furthermore, locating entities supporting C4MS within CN represents a very centralized approach and to some extent goes against a visible and well justified trend of moving as much intelligence and decision-making towards RAN / UE, which in return offloads CN. This trend is clearly visible when one analyses a leap between 2G and 3G UE. While in 2G RAN UE was merely reporting radio environment information to BSC and was completely deprived of any MM and RRM decision-making capabilities, in case of 2.5G and 3G only small – by comparison to 2G UE – fraction of radio environment information is passed towards the network.

On the other hand, achieving the same end effect in case of distributed processing of C4MS-related information will put additional overhead on the volume of exchanged information, therefore part of the gain from reduced CN processing power requirements will diminish.

Therefore additional study might be required to establish which, if any, entities supporting C4MS should reside within the CN.

Transmission of ON related data between Infrastructure Entities over the air:

The following paragraph reviews another possible implementation option for the exchange of context information, policies and ON management signalling between 3GPP network entities. The main idea of this approach is to enable the signalling over the air by using user terminals for routing signalling traffic between different network entities. The proposed approach is based on the assumption that a single user terminal can establish a connection with at least two OneFIT capable network entities. It is worth noting that this approach could reuse one of the proposed solutions introduced in section 5.5.1.1 for coordination of the infrastructure entities with the user terminals.

The user terminal in this case would be additionally responsible for relaying the signalling data between the network entities. C4MS users within the network entity could determine the proper user to route the signalling information based on the terminal measurement reports. The pros and cons, with respect to the overall pros and cons of the 3GPP based approach are listed in the table below.

Transmission of ON related data between Infrastructure Entities over the air	
Pros	Cons
• No additional Iur, Iurh, Iur-g , X2, Iu, and S1 load generated • Possible Inter-operator signalling • Possible signalling between 3GPP and non-3GPP access networks	• User terminal involvement is necessary (additional power drain, etc.) • Additional security mechanisms are required

Table 6: Advantages and Disadvantages of Transmission of ON related data between Infrastructure Entities over the air

It is worth noting that, in some cases, the proposed solution could be realized without the involvement of the user terminal. This could be the case especially with the HNBs which must support the NLM (Network Listening Mode). NLM allows a HNB to receive information broadcasted by neighbouring base stations thus could potentially allow a direct exchange of information between network entities. However, since the NLM can be used only if no user terminal is connected to the base station such variation of the proposed solution may require modifications or enhancements to NLM.

An interesting area of discussed solution is its distributed approach to C4MS information exchange. Rather than involving RAN and CN elements and resourced to carry relevant data it uses UE(s) to pass needed information. A considerable advantage of this solution is that C4MS would not need to be supported anywhere else but “close-to-RAN” so to speak and that is exactly where C4MS is expected to bring benefits. As discussed in section 5.5.1.1, an extension of Direct Transfer would be needed to enable provisioning of C4MS-related content to infrastructure entities by UE but one can speculate that perhaps only nodes (NB, eNB, hNB) would support C4MS therefore drastically reducing complexity of the solution due to:

- no need for C4MS beyond RAN entities

- no additional interfaces necessary to enable inter MNO signalling
- the same processing requirements in CN (no increase)

Furthermore, C4MS-related activity on part of the infrastructure entities would start only when necessary – that is only, when UE(s) form an ON and use an AP.

5.5.2 IEEE 802.11 based approach

5.5.2.1 Vendor Specific Information in MAC frames

The exchange of additional data in the form of C4MS PDUs between IEEE 802.11 devices, based on existing specification (see [14]), can be achieved in two different ways. The first approach makes use of the Vendor Specific information elements (VSIE) which can be included in the management frames (e.g. Beacons, Probes, Action frames).
The Vendor Specific information element (VSIE) is used to carry information not defined in the IEEE 802.11-2007 standard within a single defined format, so that reserved information element IDs are not usurped for nonstandard purposes and so that interoperability is more easily achieved in the presence of nonstandard information. The maximal size of the C4MS data which can be conveyed using this method is limited by the maximal size of the Information Element (IE) i.e. 255 octets (it is important to note that multiple VSIEs can be included in a single management frame).

The alternative approach is to use the Vendor Specific Action (VSA) frames which are stand-alone management frames. The size of the C4MS data which can be transmitted using the VSA frame in this case is limited by the maximum MMPDU size. In order to enable the data exchange between two not associated devices, Public Vendor Specific Action (PVSA) frames could be employed.

Figure 17: Vendor Specific Information Element format (top) and Vendor Specific Action Frame format (bottom) [14]

C4MS layer in the proposed approaches would be responsible for generation of properly formatted C4MS data and determining the MAC address of the destination node. The application of the proposed approaches would require interaction between C4MS layer and the IEEE 802.11 MLME layer what could be achieved via Station Management Entity (SME). It is worth noting that SME may need to be extended to enable access of C4MS entity to the specific IEEE 802.11 procedures.

Vendor Specific Information Element	Vendor Specific Action frame
Pros: • C4MS data transmitted along with beacons and other management frames Cons:	Pros: • No segmentation unless the size of maximum MMPDU is exceeded • Stand-alone management frame - No

• Only as part of 802.11 management frames • Some octets are wasted on overhead and segmenting (C4MS PDUs may be segmented) • Additional overhead in case of a repetitive transmission (other 802.11 IEs may not be required)	overhead due to the additional IEs Cons: • Large overhead in case of the exchange of small messages (L2 + L1 overhead)

Table 7: Advantages and Disadvantages of different implementation options of the IEEE 802.11 based approach

5.5.2.2 IEEE 802.11u

An alternative approach for the transmission of C4MS data in 802.11 networks could be based on the Generic Advertisement Service (GAS) described in IEEE 802.11 u "Interworking with external networks" [17]. This service allows the exchange of arbitrary information between two not associated devices using public action frames. Additionally, 802.11u describes new IEs which can be included in beacons and probe responses to carry information about the type of information (Advertisement Protocol) which is being transmitted over GAS.

The approach could be suitable to realize exchange of signalling information necessary to enable suitability determination (when the opportunistic network is not yet established) and inter-ON coordination. The additional IEs included in beacons and probe responses could be useful for the implementation of the passive and active discovery mechanisms.

In this approach C4MS layer would be responsible for generation/reception of requests and responses which are being transferred using corresponding GAS messages (i.e. GAS Initial Request, GAS Initial Response, GAS Comeback Request, GAS Comeback Response) as well as determining address of the destination node. In order to enable the transmission of C4MS data over GAS, a new Advertisement Protocol ID (see Table 7-43bi [15]) would need to be introduced.

It is worth noting that the GAS request is always followed by the GAS response what may introduce additional overhead in case the exchange of C4MS data would not require acknowledgements.

5.5.2.3 Direct Wi-Fi Approach

Another possible approach for the realization of the C4MS could be based on WiFi Direct. WiFi Direct is a new solution provided by the Wi-Fi Alliance (WFA) which is based on IEEE 802.11. The solution introduces new features/functions which extend capabilities of Wi-Fi devices and enables for the direct communication without the use of an Access Point (AP). A major improvement is the notion of software AP supported by all Direct Wi-Fi devices, which allows new group configuration and topologies. The most relevant (from the C4MS implementation point of view) WiFi direct features are related to the P2P Discovery and Group Operation functions (see Annex A.6 for more detail).

Wi-Fi Direct provides also additional information in 802.11 Wi-Fi MAC frame by using new specific Information Elements and new specific (Public) Action Frames. For instance, at the first steps of the node association in Direct Wi-Fi, additional information in VSIE is

distributed which allows P2P Devices to have a coarse (and more precise if needed) overview about the status of devices (e.g. connected or not connected to a network, ability to join a certain network) and about the P2P Groups (e.g. list of devices in the group and their capabilities). The information collected during the P2P discovery (device discovery and service discovery) procedure could be easily used during the ON lifecycle (particularly in the ON suitability determination phase). Indeed the collected information from a Group Owner or from any probe response could be provided to CSCI which then choose the best option for the ON creation. In order to provide additional ON specific information, further extension of the existing set of P2P Information Elements could be considered (see [54] for the complete list of P2P IEs). In this case, the new IEs could deliver information related to e.g.: the type of network to which each node is attached (e.g. Wi-Fi, 3GPP legacy network), the ON to which each node is attached (e.g. its services, its availability).

According to Figure 18, Direct Wi-Fi approach is to use VSIE fields to communicate. Their values are shown below:

Frame content (Octets)	Element ID (1)	Length (1)	OUI (3)	OUI type (1)	P2P Attributes (variable)
Value	0xDD (hexa)	Variable	50 6F 9A	0x09 (to be assigned)	One of more P2P attributes appears in the P2P IE.

Table 8 : Wi-Fi Direct P2P IE frame[54]

In addition, the structure of the P2P Attribute field is explained in the table below:

Frame content (Octets)	Attribute ID (1)	Length (2)	Attribute body field (variable)
Description	Identifying the type of P2P attribute	Length of the following fields in the attribute	Attribute-specific information fields

Table 9 : P2P Attributes field[54]

Attribute ID can take values in {0:255} set. The content of Attribute Body field then depends on the corresponding Attribute ID number (for the complete list of Attribute ID value please see [54], section 4.1.1).

As already described in the 802.11 paragraph, C4MS layer could be responsible for generating or encapsulating the correct formatted data.

WiFi direct provides a good framework that could facilitate the implementation of the C4MS and allow for a partial reuse of the existing procedures in other phases of ON lifecycle. One of the procedures which could be of particular relevance to the implementation of C4MS is the Group Owner Negotiation procedure which enables determination of the P2P Groups Owner as well as characteristics of the P2P Group (see [54] for more detail). The procedure could be reused, for instance, to implement the ON Negotiation procedure. Another procedure which could be potentially reused is the P2P Invitation procedure which allows P2P Group members to invite not-associated devices to join an existing P2P Group (the invitation can be issued based on different reasons).

5.5.3 WiMedia UWB based approach

The WiMedia Distributed Medium Access Control (MAC) [56] as used for Ultra-Wideband (UWB) allows a device to include a user defined data in the form of Application-specific Information Element (ASIE) in its beacon. The amount of data which can be included varies

from 0B to 320B depending on the number of additional IEs included in the beacon. WiMedia provides three different service primitives which allow addition, removal and indication of the received ASIE. The exchange of C4MS data between WiMedia terminals could be then achieved based on the Application-specific IEs. C4MS layer in this case would be responsible for the interaction with the Device Management Entity (DME) and the ASIE content management (creation, alteration, etc.).

The WiMedia standard allows definition of the application-specific command frames. The size of the application specific command frames is not limited (commands may be fragmented for the transfer between peer MAC entities [56]). The command frames are sent during data transfer period (not in the beacon period) indicating that both the transmitter and the receiver need to be active at least during one MAS. The exchange of C4MS data between WiMedia terminals can be achieved in this case using the Application-specific command frames. C4MS entity would be responsible for the interaction creation of the AS command data content.

octets: 1	1	2	N
Element ID (=255)	Length (=2+N)	Specifier ID	Application-specific Data

octets: 2	...
Specifier ID	Data

Figure 19: Application Specific Information Element format (top) and payload format for Application Specific Command frame (bottom) [56]

Application Specific Information Element	Application Specific Command frame
Pros: • Beacons are transmitted during the reserved timeslots (no channel contention) • Low power consumption (devices need to maintain active only during the beacon period) Cons: • Beacons send every 65535us (possible low responsiveness to the changes in the environment) • Limited size (320B max)	Pros: • Unlimited size Cons: • Higher power consumption (devices need to maintain active during the beacon period and at least one MAS) • Large overhead in case of the exchange of small messages (L2 + L1 overhead)

Table 10: Advantages and Disadvantages of different implementation options of the WiMedia UWB based approach

5.5.4 Bluetooth based approach

Bluetooth is a proprietary open wireless technology standard for exchanging data over short distances (using short wavelength radio transmissions[57].The C4MS data provision can be conducted based on the Extended Inquiry Response (EIR) packet, which has been introduced in Bluetooth 2.1 in order to allow better filtering of devices before connection by

providing more information about the device during the inquiry procedure. The use of EIRs allows the transmission of 240B of arbitrary data.

Another approach which could be used for the C4MS data transmission is based on the use of the Advertisement and Scan Response packets. The amount of data which can be transmitted over an Advertisement and Scan Response packet is limited to 30B. It is worth noting that although the Bluetooth specification [57] states that the Scan Response data is "generally static in nature" it does not forbid the alteration of data carried by the packet.

It is worth noting that the listed approaches for the exchange of C4MS data do not require the connection to be established (no pairing) and thus could be successfully used during the suitability determination phase.

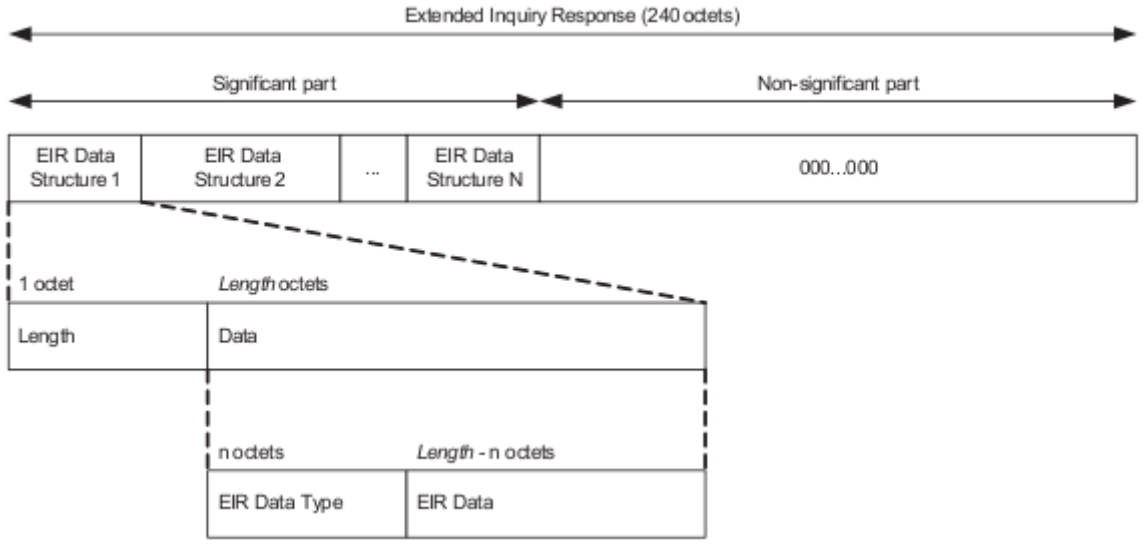


Figure 20: Extended Inquiry Response data format [57]

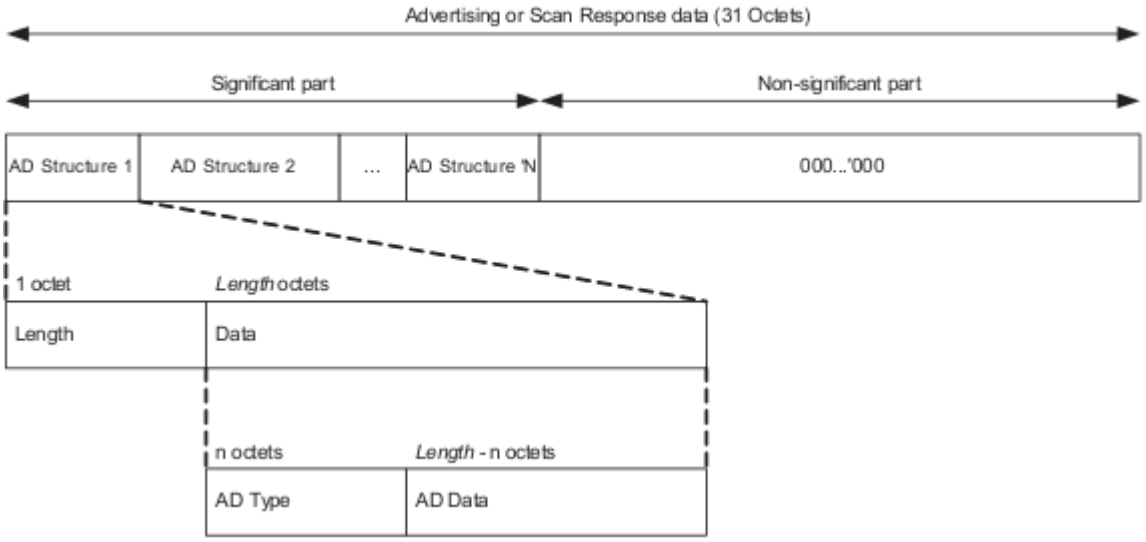


Figure 21: Advertising and Scan Response data format [57]

The realization of the C4MS data exchange in case the connection is established could be based on the Service Discovery Application Profile (SDAP). The basic idea of the approach is to use Service Records which describe specific service (in our case the service could be called C4MS) to represent the C4MS data (e.g. ON specific parameters, context information,

policies), making it accessible to other devices in the neighbourhood. It is worth to note that the Bluetooth specification allows users to defined new service attributes (see Volume 3, Part B, section 2.3).

Extended Inquiry Response, Advertisement/Scan Response	Service Discovery Application Profile
Pros: • Connection establishment is not required (no pairing) Cons: • Limited size (especially in case of Advertisement/Scan Response) • Increased probability of error due to interference (especially in case of Extended Inquiry Response)	Pros: • Unlimited size Cons: • Requires connection to be established (pairing is required) • High delay (compared to the Extended Inquiry Response)

Table 11: Advantages and Disadvantages of different implementation options of the Bluetooth based approach

6. Technical challenges

6.1 Challenges related to the implementation of the C4MS over existing interfaces/protocols

The Table 12 presents a summary of the C4MS-NET-SAP implementation options that have been detailed in the chapter 5.4 and 5.5.

CM4S protocol options	Ending points		User plane				Adressing
			Layer 1, Layer 2	Layer 3	Layer 4	Protocol	
System/RAT independant							
Diameter	Eqt 1	Eqt 2	NR	IP	TCP, SCTP	Diameter	IP network
IEEE 802.21	Eqt 1	Eqt 2	NR	IP	TCP, UDP, SCTP	MIH	IP network
ANDSF	UE	ANDSF	NR	IP	TCP	HTTP, OMA-DM (XML)	IP network
Distributed agent	Agent	Agent	NR	IP	TCP	HTTP, Corba/IIOP	IP network
TR069	CPE	ACS	L1,L2	IP	TCP	HTTP-SOAP	IP network
SNMP	Eqt 1	Mgt	L1, L2	IP	UDP	SNMP	IP network
System/Rat dependant							
3GPP							
UE-Core Network	UE	eNodeB	L1,L2	RRC	-	RRC	IMSI/TMSI, RNTI
eNodeB <->eNodeB	eNodeB	eNodeB	L1, L2	IP	SCTP	X2AP	IP private operator network
eNodeB <-> RNC	eNodeB	RNC	L1, L2	IP	SCTP	RNSAP	IP private operator network
802.11	AP/STA 1	STA 2	802,11	-	-	802.11	MAC address
802.11 Direct wifi	STA 1	STA 2	802,11	-	-	802.11	MAC address
Wimedia	Eqt 1	Eqt 2	L1, L2 (UWB)	-	-	ECMA-368	MAC address
Bluetooth	Eqt 1	Eqt 2	L1, L2	-	-	Bluetooth 2.0	MAC address
NR : Not relevant							

Table 12: C4MS implementation options

The Figure 22 presents the existing interfaces and considered protocols for the C4MS communication options. The figure was build from the system architecture considered by the project. Those interfaces and protocols are forming the baseline to be considered for C4MS implementation options.

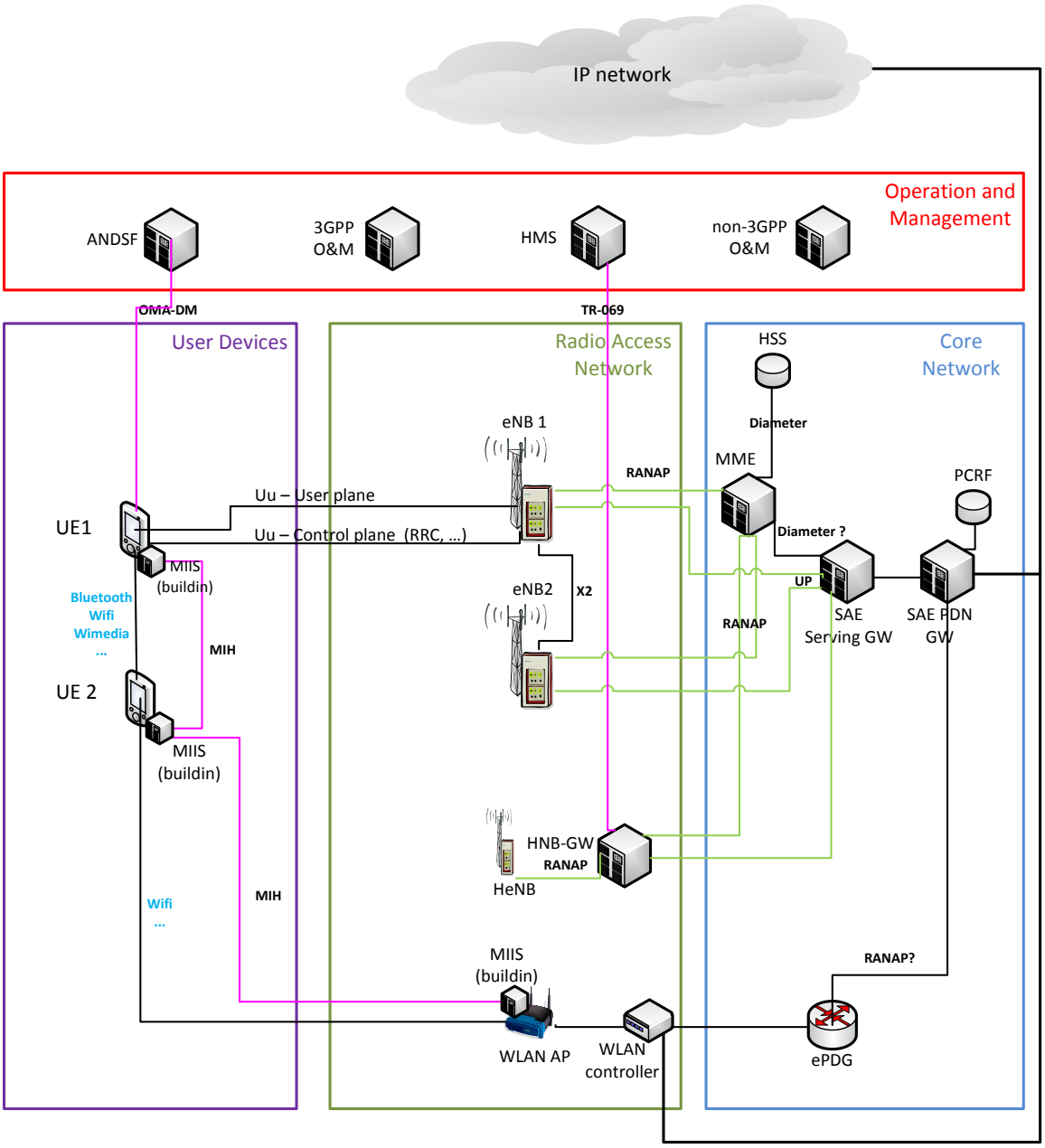


Figure 22: C4MS Communication protocol baseline

The Figure 22 shows that various protocols already exist in the entities supporting C4MS users.

- Layer 1&2 : Many different types of layer 1 and 2 are existing and are depending on the entities considered,
- Layer 3/4 : most of the entities are communicating over IP, using UDP, TCP or SCTP transport protocols,
- Layer above 4: several protocols have been identified (RNSAP, Diameter, OMA-DM, TR069) are identified, but are used only between specific entities.

Section 5 presented a reference model of the C4MS. As seen, the C4MS-NET SAP support 2 different communications services :

- C4MS message over U-Plane
- C4MS message over C-Plane

6.1.1 C4MS communication over C-Plane

When no U-Plane is established, then, C4MS Communication over C-plane is possible. This will be used for example when UE is out of coverage for discovering the neighbour C4MS.

When U-Plane is established, the communication between C4MS users can be done either using the C-Plane, or using the U-Plane.

When U-Plane is established, it remains possible to use only C-Plane for C4MS communication. This is expected to be challenging in this case due to the fact that:

- A full routing layer has to be designed for ensuring the addressing, forwarding, broadcast, multicast requirements of C4MS between entities, typically UEs, that are not linked by any C-Plane in the legacy 3GPP networks
- This is complexified due to the various different C-plane protocols existing and depending on the C4MS entities.

6.1.2 C4MS communication over U-Plane

When U-Plane is established, and due to the C4MS communication requirements, it can be expected that most of the C4MS service like discovery, message forwarding, addressing, broadcast, are realised by using the IP protocol capabilities.

Anyway, the IP U-Plane address scheme in the system architecture considered in the project is unlikely to be straitfully usable due to the following issues :

- A UE cannot communicate with network equipements like eNodeB, HeNB. UE IP address is allocated by the Serving GW. ENodeB and HeNB are using IP adresses that are private to the operator network.
- IP network capabilities for broadcast is possible inside an IP network subnet. To use the broadcast capabilities of IP for broadcasting a C4MS message in an ON, the OneFIT must define a complete management for transitory and private IP sub-network.

An alternative solution could be that the IP network capabilities are not used for realising the C4MS service service like discovery, forwarding, addressing, broadcast, unicast, multicast. In this case a full routing layer has to be designed for ensuring the addressing, forwarding, broadcast, multicat requirements of C4MS.

6.2 Challenges related to transported information

The information transported by C4MS is required either for feeding decision making or configuration of distant nodes.

This information is completely linked to the needs of the algorithms for the management of ONs.

The identification of this information cannot be complete and future-proof at this stage, as the work in OneFIT WP4 is only starting, but also at the end of the project, future enhanced algorithms may require different information.

C4MS then must offer easy and future-proof extensibility.

6.3 Challenges related to performance

The use of an unknown number of relays for carrying the signalling introduces some uncertainties in the delay that the procedures will have to be robust to.

The fact that the different hops could be with different RAT introduces additional uncertainty.

The option of using protocols on top on IP layer has the drawback of having long propagation delays which may be incompatible with some very short-term reaction times, e.g. form maintenance of the ON: anticipation mechanisms and autonomous decision/behaviour may need to be designed to cope with such situations.

In the same way, the mobility of relays introduces the risk of loss or duplication of signalling, which will have to be taken into account in routing policies for signalling and error management in procedures.

Finally, the dynamics and volume of the signalling, which is a usual tricky point of using higher layer, will have to be carefully evaluated to ensure that the signalling alone is not consuming a large part of the bandwidth available at each hop.

6.4 Challenges related to standardisation

The ON management designed by OneFIT is aimed at running over/in 3GPP-based operator networks.

These networks are built on strong standard specifications and there is an enormous legacy both in the specifications and the actual implementations/deployments.

Any ON-related evolution will have to fit into existing specification framework and concepts to be acceptable by the 3GPP eco-system.

6.5 Challenges related to regulation

Opportunistic networks introduce an innovative way to use spectrum more efficiently in order to provide users increased QoS for their applications or to provide services in areas they were not available before. The use of spectrum is mandated by national and international regulation and therefore it is important to have knowledge of the regulatory framework in order to ensure that the solutions created are possible and in accordance with it. It is also possible to influence regulation.

6.6 Challenges related to security and trust

The Security and Trust requirements for ON management are still under work. It is foreseen that "native" security obtained through RAT/CN-specific procedures will provide the basis for the complete Security framework. As additional procedures are likely to be needed, they may be, either based on existing 3GPP mechanisms, or built as an additional Public Key-based scheme. The rest of this section identifies the potential challenges related to such an additional Public Key-based scheme.

Accessability and presence of a trusted third party (TTP) which would be responsible for issuing the certificates.

Integration and effective usage of multiple existing security mechanisms provided by different systems that can be potentially a part of an ON.

Security and trust related mechanisms introduce additional communication and computational overhead which needs to be taken into account. Various solutions which could minimize this overhead needs to be considered and carefully analyzed.

Security and trust related mechanisms need to address the problem of internal attacks such as various selfish behaviours (e.g. dropping of relaying packets), sending false C4MS messages (e.g. false context information), saturation of the C4MS (e.g. injecting a large number of C4MS messages to disturb signaling). This requires implementation of different mechanisms for monitoring node's behaviour as well as key revocation and key renewal shemes. The key revocation sheme needs to be also robust against false accusation attacks which may lead to revocation of keys of honest nodes.

7. Conclusions

This document provided the "Control Channels for the Cooperation of Cognitive Management Systems" (C4MS) proposal for further analysis, development and specification within OneFIT WP3. The proposal is based on the the combination of Cognitive Pilot Channel (CPC), Cognitive Control Channel (CCC) and Cognitive Control Radio (CCR) concepts and can be seen as a first step towards the actual implementation of the C4MS. The document identifies a number of various implementation options, including RAT/System independent and RAT/System dependent approaches. The analysis provided in the document shows that the various options for implementation of the C4MS have different advantages and drawbacks. The RAT/System independent based solutions, for example, are quite generic but may lead to limitations for time critical applications. The RAT/System dependent based approaches, on the other hands, are expected to represent a low-latency solution while they need to be tailored to a specific system. It is thus expected that the final implementation of the C4MS will be adopted building on a combination of several of the above-mentioned approaches. A hybrid implementation should guarantee the most suitable solution for the delivery of infrastructure governed guidance/assistance information towards the Oportunistic Networks and for providing means for the management of Opportunistic Networks.

Additionally, the document provided a preliminary set of high level elementary procedures and related messages for C4MS protocol(s) which have been derived based on the MSCs developed in D2.2 [3]. This work can be seen as a first step prior to the development of the final set, which will be fully addressed in the future work. The document provided also first concise definitions of possible parameters/information which is to be exchanged between cognitive management systems over C4MS. The identified parameters/information provide input towards creation of the algorithms for different phases of an ON. Parameters/information will also be updated in a close collaboration with the algorithm work.

Based on the C4MS proposal, detailed technical challenges which will be fully addressed in the future work have been derived. The derived technical challenges suggest that a number of issues still need to be resolved before the actual deployment of the C4MS.

The input towards integrating an ON into a OneFIT platform is delivered by indicating different possible C4MS implementation options as well as by identifying detailed requirements and technical challenges related to the actual implemention of the C4MS.

8. References

[1] ICT-2009-257385 OneFIT Project, http://www.ict-onefit.eu/

[2] OneFIT Deliverable D2.1 “Business scenarios, technical challenges and system requirements”, October 2010

[3] OneFIT Deliverable D2.2 “OneFIT functional and system architecture”, February 2011

[4] 3GPP TS 22.278 "Universal Mobile Telecommunications System (UMTS); LTE; Service requirements for the Evolved Packet System (EPS) (Release 8)"

[5] 3GPP TS 23.402 "Universal Mobile Telecommunications System (UMTS); LTE; Architecture enhancements for non-3GPP accesses (Release 8)"

[6] 3GPP TS 24.312 "Universal Mobile Telecommunications System (UMTS); Access Network Discovery and Selection Function (ANDSF) Management Object (MO) (Release 8)"

[7] 3GPP TS 25.413, "UTRAN Iu interface Radio Access Network Application Part (RANAP) signalling", v10.0.0

[8] 3GPP TS 25.423, “UTRAN Iur interface Radio Network Subsystem Application Part (RNSAP) signalling”, v10.0.0

[9] 3GPP TS 29.229 “Cx and Dx Interfaces based on Diameter protocols; protocol details”

[10] 3GPP TS 32.583 “Home Node B (HNB) Operations, Administration, Maintenance and Provisioning (OAM&P); Procedure flows for Type 1 interface HNB to HNB Management System (HMS) (Release 9)”

[11] 3GPP TS 33.102 “3G Security; Security Architecture”

[12] 3GPP TS 36.331 “Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification

[13] 3GPP TS 36.413, "Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP)", v10.0.0

[14] IEEE Std 802.11–2007 IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks-Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

[15] IEEE 802.11u: Part 11 Amendment 9: Interworking with external networks, February 2011

[16] IEEE 802.19 system Description and Reference Model - https://mentor.ieee.org/802.19/dcn/10/19-10-0055-03-0001-system-design-document.doc

[17] IEEE Std 802.21TM-2008, “IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services.”, IEEE Computer Society, Sponsored by the LAN/MAN Standards Committee, January 2009

[18] IEEE Std 802.21-2008, IEEE Standard for Local and Metropolitan Area Networks Part 21: Media Independent Handover Services, IEEE, January 2009.

[19] IEEE 1900.4 Standard for Architectural Building Blocks Enabling Network-Device Distributed Decision Making for Optimized Radio Resource Usage in Heterogeneous Wireless Access Networks, Feb. 27, 2009

[20] IEEE P1900.4 Website, http://grouper.ieee.org/groups/scc41/4/index.htm

[21] IEEE P1900.5 Website, http://grouper.ieee.org/groups/scc41/5/index.htm

[22] IEEE P1900.6 Website, http://grouper.ieee.org/groups/scc41/6/index.htm

[23] IEEE std 802-1990 IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture

[24] IEEE Organizationally Unique Identifier web site http://standards.ieee.org/develop/regauth/oui/

[25] IETF RFC 2246 “The TLS Protocol Version 1.0”, January 1999

[26] IETF RFC 2401 “Security Architecture for the Internet Protocol”, November 1998

[27] IETF RFC 3413 “Simple Network Management Protocol (SNMP) Application”, December 2002

[28] IETF RFC 3588 “Diameter Base Protocol”, September 2003

[29] IETF RFC 3589 “Diameter Codes for 3GPP Release 5”, September 2003

[30] IETF RFC 5677, “IEEE 802.21 Mobility Services Framework Design (MSFD)”

[31] ETSI TR 102 683 Technical Report, Reconfigurable Radio System (RRS), Cognitive Pilot Channel (CPC), 08-2009

[32] ETSI TR 102 682 “Functional Architecture for the Management and Control of Reconfigurable Radio Systems”

[33] Open Mobile Alliance (OMA), http://www.openmobilealliance.org/

[34] OMA-ERELD-DM-V1-2: "Enabler Release Definition for OMA Device Management”

[35] Broadband Forum http://www.broadband-forum.org/

[36] TR-069 Amendmend 2 “CPE WAN Management Protocol v1.1”, Broadband Forum, December 2007

[37] Wikipedia: http://en.wikipedia.org/wiki/OMA_Device_Management

[38] “Resource Description Framework (RDF): Concepts and Abstract Syntax”, W3C Recommendation 10 February 2004. Available online at http://www.w3.org/TR/rdf-concepts/

[39] S.Buljore, H.Harada, P.Houze, K.Tsagkaris, O.Holland, S.Filin, T.Farnham, K.Nolte, V.Ivanov, “Architecture and enablers for optimized radio resource usage in heterogeneous wireless access networks: The IEEE 1900.4 Working Group” Communications Magazine, IEEE, Vol 47, no. 1, pp. 122-129, January 2009

[40] ICT-2007-216248 E3 Project, http://www.ict-e3.eu/

[41] E3 White Paper “Support for heterogeneous standards using CPC”, 30-06-2009

[42] E3 Deliverable D2.3 “Architecture, Information Model and Reference Points, Assessment Framework, Platform Independent Programmable Interfaces”, September 2009

[43] E3 Deliverable D4.4 “Final solution description for autonomous CR Functionalities”, September 2009

[44] E3 Deliverable D5.4 “Final report on Design of the CPC and coexistence of heterogeneous standards”, December 2009

[45] K. Kalliojärvi, J. Pihlaja, A. Richter and P. Ruuska, “Cognitive Control Radio (CCR) – Enabling Coexistence in Heterogeneous Wireless Radio Networks.” Proceedings of the ICT Mobile Summit 2009.

[46] Foundation for Intelligent Physical Agents (FIPA), Web site, http://www.fipa.org, accessed October 2010

[47] Java Agent DEvelopment Platform (JADE), Web site: http://jade.tilab.com, accessed October 2010.

[48] JADEX Projects, http://vsis-www.informatik.uni-hamburg.de/projects/jadex/, accessed October 2010

[49] ORBacus, IONA Technologies, http://www.orbacus.com/

[50] ICT-216856 Aragorn Project, http://www.ict-aragorn.eu/

[51] Aragorn Deliverable D3.3, “Final System Architecture”, May 2010

[52] A. Galani, K. Tsagkaris, N. Koutsouris, P. Demestichas, "Design and assessment of functional architecture for optimized spectrum and radio resource management in heterogeneous wireless networks", International Journal of Network Management, John Wiley & Sons, Vol. 20, Issue 4, pp. 219–241, July/August 2010

[53] V. Stavroulaki, N. Koutsouris, K. Tsagkaris, P. Demestichas, "A Platform for the Integration and Management of Cognitive Systems in Future Networks", in Proceedings of IEEE Globecom 2010, International Workshop on Management of Emerging Networks and Services (IEEE MENS 2010)

[54] Wi-Fi Peer-to-Peer (P2P) Technical Specification v1.1

[55] Wi-Fi CERTIFIED Wi-Fi Direct white paper 2010

[56] WiMedia Alliance, "DISTRIBUTED MEDIUM ACCESS CONTROL (MAC) FOR WIRELESS NETWORKS", MAC SPECIFICATION: RELEASE 1.5, December 1, 2009

[57] Bluetooth Special Interest Group, "BLUETOOTH SPECIFICATION Version 4.0", 2010

A Appendix: State of the Art

A.1 Cognitive Pilot Channel (CPC)

In the context of Cognitive Radio, a crucial point to enable optimisation of radio resource usage is, for a terminal, to obtain the knowledge of its radio environment, in order to switch to the most appropriate available technology and frequency.

In order to obtain knowledge of its radio environment, the terminal could use spectrum sensing, but this could be a very time- and power-consuming operation.

To tackle this problem, previous E3 research studies have defined the concept of a "CPC" (Cognitive Pilot Channel)[44] which is a kind of common pilot channel aiming at providing the necessary information for the terminal to get the knowledge of radio spectrum.

The E3 project then defines the CPC as a logical or physical channel connecting cognitive radios and cognitive networks with the aim of conveying necessary information to supply cognitive terminals with information on available frequency bands, RATs, services, load situation, network policies, etc at different geographical locations to facilitate the CR System operations. The CPC is also defined in the ETSI TR 102 683 [31].

A.1.1 CPC design

From deployment point of view, a cellular approach is used to describe CPC coverage area and from an architectural point of view, a possible solution consists in a CPC server assumed to be available somewhere in the network, offering the database functionalities needed for storing and managing the information to be conveyed throughout the CPC Information broadcast.

A.1.1.1 CPC Content

There is a need to organize the information delivered over the CPC according to the geographical area where this information applies. This section describes the methods of geographically-related information broadcast. Two methods have been proposed to solve possible problem which can be encountered, e.g spectrum bandwidth used by the CPC bearer.

A.1.1.1.1 Mesh based approach

In this approach, the CPC operates in a certain geographical area subdivided into meshes. A mesh is defined as a region where certain radio electrical commonalities can be identified (e.g. a certain frequency that is detected with a power above a certain level in all the points of the mesh, etc.). The mesh is univocally defined by its geographic coordinates, and its adequate size would depend on the minimum spatial resolution where the above commonalities can be identified. Furthermore, two methods exist for information coding in order to reduce the bandwidth, which are "CPC differential coding" and "Factorised-CPC". See [44] for more details.

The message delivered by the CPC for each mesh of the area could contain the operators available at that mesh, their preferred technologies and the corresponding frequency bands as described in the schema below:

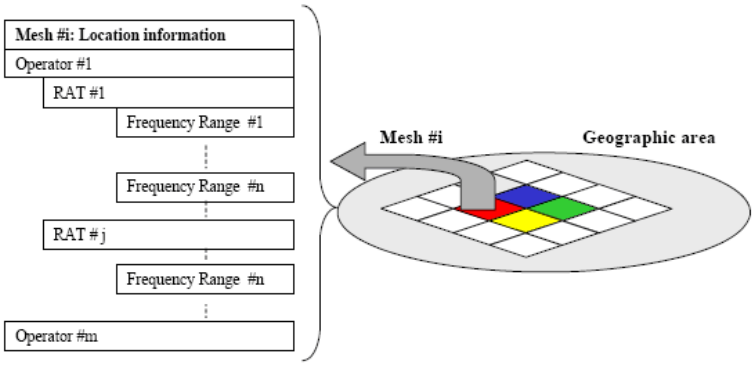


Figure 23: CPC message content with mesh approach

A.1.1.1.2 Coverage area approach

The CPC content is organised taking into account the area, under-laying CPC umbrella, where such information has to be considered valid.

It is worth to be noted that knowing the position of the mobile terminal is not a strict requirement for the CPC operation using this approach, but a capability that enables higher efficiency in obtaining knowledge:

- in case positioning is not available, as long as the mobile terminal is able to receive the CPC information, the information about the different regions in that area are available;
- in case positioning is available, a subset of the information at the actual position could be identified. The mobile terminal could then use that information.

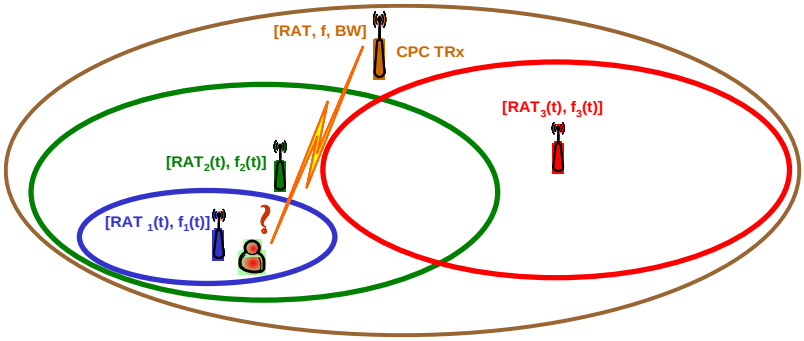


Figure 24 : Example of coverage area approach

The structure of the broadcast CPC message defined in E3 using this approach is reported in Figure 9. The concept of mesh is no more a pillar in defining the CPC content, and *a coverage area of validity* is provided:

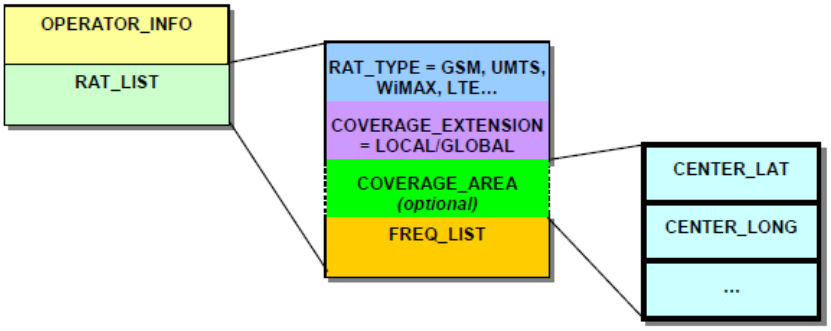


Figure 25 : CPC message structure for coverage approach

The following fields are considered in the CPC broadcast message structure:

- **Operator information**: operator identifier. This information is repeated for each Operator to be advertised by the CPC.
- **RAT list**: for each operator, provide information on available RATs. This information is repeated for each RAT of i-th Operator.
    - **RAT type**: could be "GSM", "UMTS", "CDMA2000", "WiMAX", "LTE"…
    - **Coverage extension**: could be GLOBAL (i.e. wherever the CPC is received) or LOCAL (i.e. in a area smaller than CPC coverage, to be specified)
    - **Coverage area**: to be provided in case of LOCAL coverage (e.g. reference geographical point).
    - **Frequency information**: provide the list of frequencies used by the RAT.

A.1.1.2 Deployment options

Two CPC deployment options can be considered for exchanging information between the terminal and the network. They can include the re-use/extension of existing systems.
The first one, out-band CPC, considers that a channel outside the bands assigned to component RAT provides CPC service. The second one, in-band CPC, uses a transmission mechanism (e.g. logical channel) within the technologies of the heterogeneous radio environment to provide CPC services.

A.1.1.2.1 In band

The "In-band" CPC is a CPC conceived as a logical channel within the technologies of the heterogeneous radio environment. In this case the CPC is transmitted using specific channels of the existing access technologies, e.g. the CPC could be a logical channel within one or some of the RATs available in a heterogeneous radio environment. Notice that in this context, the in-band CPC can provide both downlink as well as uplink information transfer.
The in-band CPC does not require a new frequency to be agreed and harmonized as far as it uses existing infrastructure. In that sense, some possibilities would be to use some default worldwide de-facto standard RATs, like e.g. GSM or UMTS, to convey CPC, mapping it on a logical channel. Refer to [41], [42] for more details.

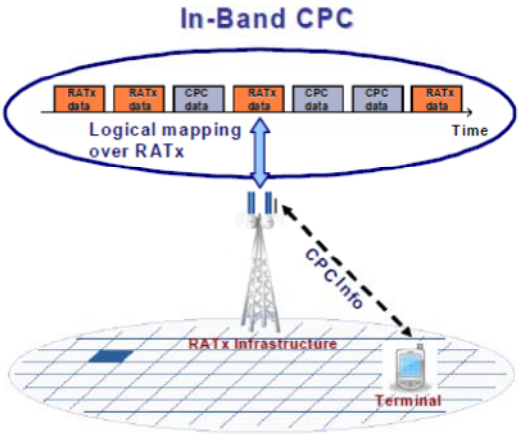


Figure 26 : In Band representation

A.1.1.2.2 Out band

The "Out-band" CPC is a CPC conceived as a radio channel outside the component RAT. In the Out-band solution, the CPC either uses a new radio interface, or alternatively uses an adaptation of legacy technology with appropriate characteristics.
The re-use of already existing RATs (or the relevant parts of them) would seem to be a valuable alternative in order to identify the CPC access technology.
A couple of possible solutions to re-use the already existing RATs were investigated which includes considering the GSM system as bearer or using Wi-Fi connectivity. Information delivery strategies for Out-band solution consist of two types: broadcast or on demand. Refer to [41], [42] and [31] for more details.

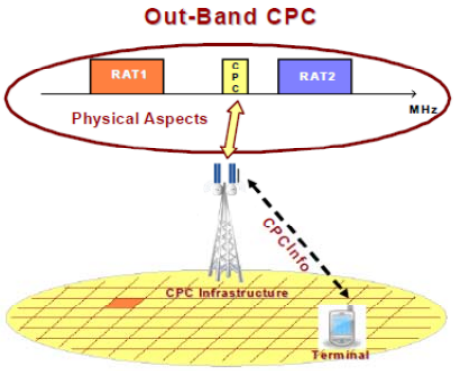


Figure 27 : Out band representation

A.1.2 Scenarios

Thanks to the deployment of the CPC, the following two scenarios can be supported by a network:

- Support for a terminal at start-up phase
- Secondary spectrum usage
- Spectrum optimization

A.1.2.1 Support for a terminal at start-up phase

In a future scenario where regulation allows Dynamic Spectrum Allocation and Flexible Spectrum Management, a terminal may have no knowledge on which Radio Access Technologies are available at which frequencies. In such a scenario, an out-band CPC on a well defined frequency can provide information about available operators, RATs and frequency ranges in a given geographic area [31]

A.1.2.2 Secondary spectrum usage

In this case, a bi-directional out-band CPC is used to assist in establishing a secondary spectrum usage communication. In this case, CPC participates in three procedures:

- Acquiring initial information on frequency bands for secondary usage: during acquiring initial information on frequency bands allowed/available for secondary usage, CPC operates as downlink broadcast channel, similar to the start-up scenario.
- Assisting in spectrum sensing: during assisting in spectrum sensing, out-band CPC operates as bi-directional channel. As such it is used by secondary base stations and terminals to exchange spectrum sensing information, including control information coordinating measurement schedule, raw/processed measurements, and detection decisions/results.
- Assisting in secondary system start-up.

A.1.2.3 Spectrum optimization

The CPC can be used for collaborative radio resource usage optimization by providing means to exchange context information between network and terminals and providing policies to terminals. This assists in decision making and reconfiguration of network and terminals.

A terminal may receive information delivered by the out-band CPC. When the terminals have some level of connection with a network, the in-band CPC can be used. Generally, an in-band CPC is bi-directional and information to be exchanged is much more detailed and dynamic than the one broadcasted over out-band CPC. Consequently, for this purpose, an in-band CPC could be a more technically efficient solution compared to an out-band CPC.

A.2 Cognitive Control Radio

The purpose of Cognitive Control Radio (CCR) is to enable distributed, inter-system, inter-technology control mechanisms and to provide means to exchange control information between nodes and networks in a heterogeneous environment [43]. CCR connects nodes of different networks using different radio technologies on different bands and by doing that creates a network of networks. The CCR is a complementary concept to CPC, which targets to solve the same problem with centralized approach. Functionalities of CCR include

- finding availability information of networks, radio access technologies, and services,
- negotiating local spectrum usage between networks,
- facilitating cooperative spectrum sensing and
- disseminating local spectrum regulations and policies.

The most efficient way to implement CCR is as a real physical (outband) channel operating on a frequency band preferably dedicated solely for it. This way, new nodes are not required to search first for the CCR operating frequency and there is not a risk that multiple independent CCR networks would exist in the same local area. However, the CCR can also be established with decreased reliability e.g. in an ISM band or even in white spaces. In each network connected with the CCR, there needs to be at least one node actively connected to the CCR network. In addition, there needs to be mechanisms to disseminate control messages in the CCR network. This can be done e.g. by an inband version of the CCR, Cognitive Control Channel, which is further described in Appendix A.3.

A.3 Cognitive Control Channel

Cognitive Control Channel (CCC) was introduced in E3 project [40] as an alternative solution to Cognitive Control Radio (CCR). CCC was proposed to address the scenarios in which cognitive control information needs to be distributed without the CCR connectivity. Similarly to CCR, CCC targets the exchange of cognitive information which is relevant to other secondary nodes in the area. CCC can be defined as a logical channel thus can be realized over CCR as well as CRN links. The usage of CCC has been illustrated on Figure 28. It is worth to point out that the focus of the E3 project was on CCR and CPC thus not much work was done with respect to CCC.

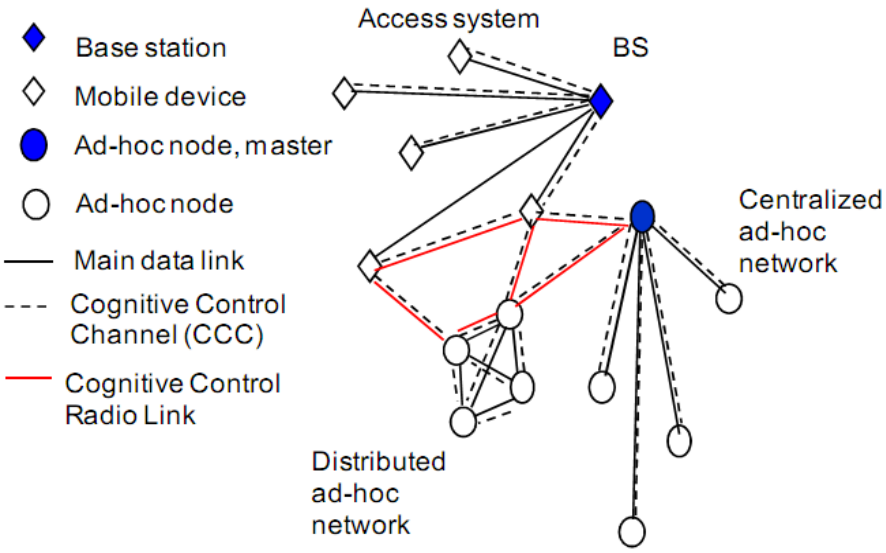


Figure 28: CCC operating on CCR links and CRN link [42]

A similar solution has been proposed in the on-going project called Aragorn [50]. The solution within the project is interchangeably called Common Control Channel or Common Communication Channel and has been introduced to enable the application of different resource optimization algorithms which require collaboration between different nodes. The proposed conceptual architecture of CCC in Aragorn is depicted in Figure 29:

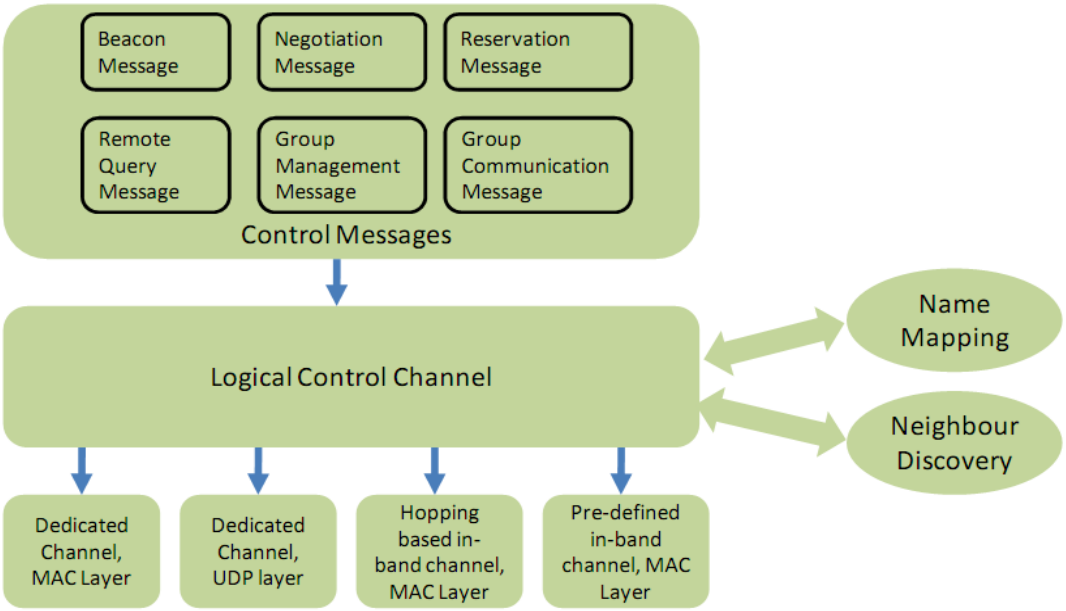


Figure 29: Conceptual Architecture for the Common Control Channel [51]

The main part of the proposed concept is the Logical Control Channel (LCC) layer which provides the CRM (Cognitive Resource Manager) with access to different services which are necessary to enable the successful control message exchange between the nodes. The main service provided by LLC allows CRM to send and receive control messages from/to control channels. The other main services are the name mapping service and neighbour discovery service. The name mapping service is used to map the name of the sender/receiver to a specific identifier assigned to the underlying physical control channel. The neighbour discovery service allows CRM to identify nodes in the vicinity (the procedure is conducted for all the available network interfaces). According to the authors, the neighbour discovery service, upon request, shall also provide information which is relevant for CCC setup and data exchange (e.g. channel occupancy)[51].

The control channels which are located under the LCC have been subdivided in two groups: 1) Dedicated Control Channels and 2) In-Band Control Channels. The first group makes use of dedicated resources (i.e. dedicated RAT) to transport control information between the nodes. The second group uses the same resources for control and data information exchange. Different implementations for dedicated as well as in-band control channel are suggested (e.g. Transport layer based, MAC layer based)[51].

The conceptual communication layer architecture of the ARAGORN system can hence be represented as in Figure 30.

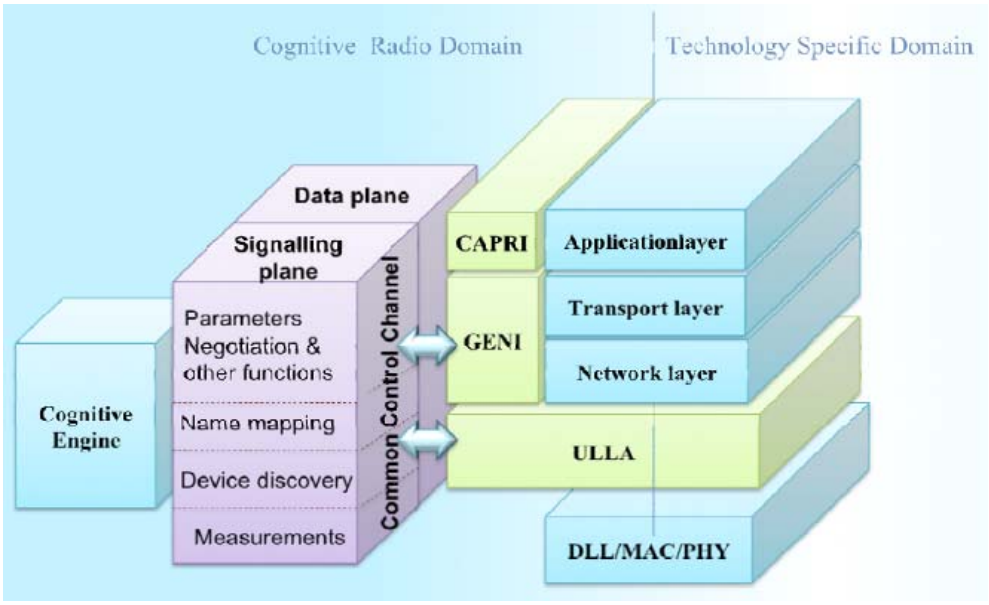


Figure 30: The conceptual communication layer architecture of the ARAGORN system [51]

A.4 Open Mobile Alliance (OMA) Device Management (DM)

The OMA Device Management (DM)[34] is specified by the Open Mobile Alliance (OMA)[33] and is designed for the management of small mobile devices such as mobile phones, PDAs and palm top computers. The OMA DM uses the OMA SyncML Common Specification which defines an XML-based representation protocol, a synchronization protocol and a device management protocol.

The device management is intended to support [37]:

- Provisioning – Configuration of the device (including first time use), enabling and disabling features
- Configuration of Device – Allow changes to settings and parameters of the device
- Software Upgrades – Provide for new software and/or bug fixes to be loaded on the device, including applications and system software.
- Fault Management – Report errors from the device, query about status of device

The OMA DM was originally developed by the SYNCML Initiative, an industry consortium formed by many mobile device manufacturers. The SyncML Initiative got consolidated into the OMA umbrella as the scope and use of the specification was expanded to include many more devices and support global operation.

The SyncML Common representation, synchronization and device management protocols are transport-independent. However, the SyncML Common specification defines transport bindings that specify how to use a particular transport to exchange messages and responses,. Each package in these protocols is completely self-contained, and could in principle be carried by any transport. The initial bindings specified are HTTP, WSP and OBEX as shown in Figure 31, but there is no reason why SyncML Common could not be implemented using email or message queues, to list only two alternatives.

Sync ML			
HTTP	HTTPS SSL/TLS	WSP	OBEX
TCP/IP	TCP/IP	WAP	USB, Bluetooth, ..

Figure 31: OMA DM Protocol Transport Options

A.5 3GPP Access Network Discovery and Selection Function (ANDSF)

The scope of the 3GPP Access Network Discovery and Selection Function (ANDSF) is to support multi-access network scenarios with intersystem-mobility between 3GPP-networks (GSM, UMTS, LTE) and non-3GPP networks (e.g. WiMAX, WLAN) [5]. The ANDSF is located in the 3GPP Evolved Packet Core (EPC). The ANDSF provides inter-system mobility policies and access network specific information from the network to the user equipment (UE) in order to assist the mobile node for performing the inter-system handovers. This set of information can either be provisioned in the UE by the home operator, or provided to the mobile node (MN) by the ANDSF [5] . In 3GPP release-8, the ANDSF is located in the subscriber's home operator network (H-ANDSF) as shown in Figure 32 while in 3GPP release-9, the ANDSF can also be located in the visited network (V-ANDSF).

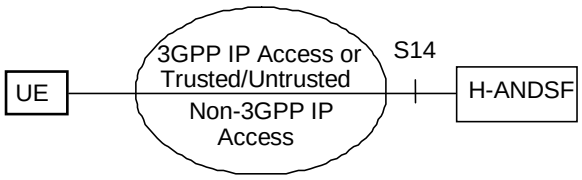


Figure 32: Non-Roaming Architecture for Access Network Discovery Support Functions[5]

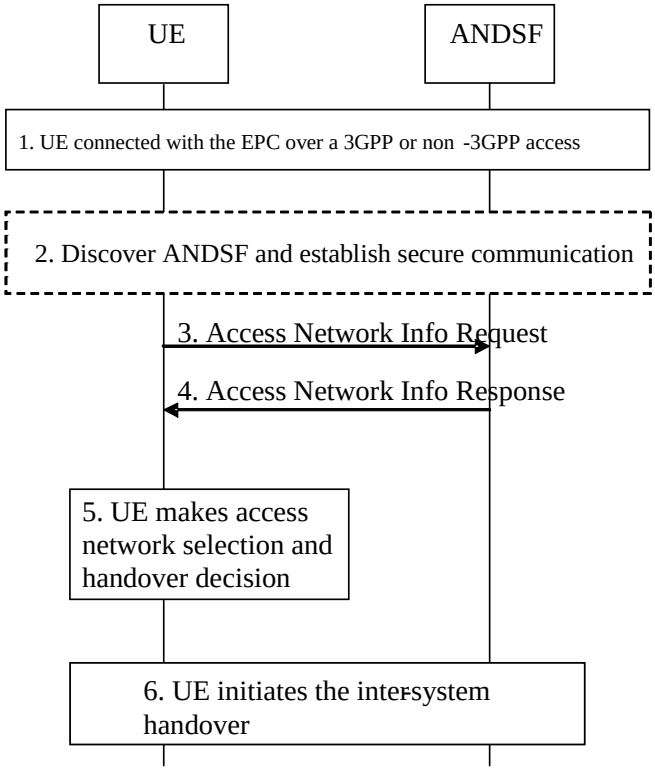


Figure 33: Handover between 3GPP Access and trusted / untrusted non-3GPP IP Access with Access Network Discovery and Selection [5]

The information distributed between the ANDSF and the UE is defined in the ANDSF MO (Management Object)[6] which is compatible with the OMA Device Management (DM) protocol specifications[34] as described in section A.4 before.

A.6 Wifi Direct

Direct Wi-Fi is a new solution given by the Wi-Fi Alliance (WFA) which is based on IEEE 802.11[54]. Direct Wi-Fi is Wi-Fi compatible, it introduces new features which extend Wi-Fi devices capabilities. A major improvement is the notion of software AP supported by all Direct Wi-Fi devices, which allows new group configuration and topologies

While Wi-Fi Direct is completely compatible with certified IEEE 802.11 technology, WFA added specific functions for devices. These new functions include:

- **Group Operation**: resembles infrastructure BSS operation as defined in [14], and provides additions for a P2P Group operation. This function includes possibility of Group Creation with Wi-Fi Direct devices or WFA certified devices for specific services such as Connection sharing, the use of Persistent Group (re-invoked P2P group after initial termination), Concurrent connection (Capability of a Wi-Fi Direct Device to maintain multiple connections simultaneously. Connections can be to Groups and/or traditional WLAN) in order to provide infrastructure access to other device in the group.
- **Power Management**: provides a set of functions to reduce power consumption of P2P Devices. The P2P Specification includes power management mechanisms that can reduce power consumption for devices regardless of role within a Group, while maintaining valuable discovery capabilities by using the Notice of Absence mechanism and Opportunistic power saving.

The Architecture of Wi-Fi Direct is based on 2 kinds of components:

- **P2P Group Owner**: AP-like entity that provides 802.11 Base Service Set (BSS) functionality (see [14]) and services for associated Clients (P2P Clients or Legacy Clients). It may provide communication between associated clients or access to other WLAN connection to the associated clients.
- **P2P Client**: Implements non-AP Station (STA) functionality

P2P Devices stands for generic device name in Wi-Fi Direct architecture. Thus, among all its functionalities, we can emphasize that:

- It supports both P2P Group Owner and P2P Client roles.
- It may support WLAN and P2P concurrent operation

According to the terms defined above, Wi-Fi Direct devices can form group called **P2P Group**.

Moreover, Wi-Fi Direct specification adds the notion of Concurrent Operation in which a P2P Device can operate concurrently with a WLAN (infrastructure network) as shown in the figure below. Such device is called **P2P Concurrent Device**.

Direct Wi-Fi specificity is to allow all certified devices to have the Client Role or the Group Owner Role, depending on the scenario. All Direct Wi-Fi devices have P2P Device capacities. Unlike Wi-Fi, this flexibility, added these new functions and capabilities related to a certified

Direct Wi-Fi device (see Table 13 and Table 14 for a global view), allows formation of groups with different topologies and new capabilities e.g. connection sharing, cross-connection or persistent group.

A.6.1 Discovery Processes

Discovery in Direct Wi-Fi follows the same logical process as in classical Wi-Fi. However, new processes and functions are added to simplify the discovery. The main addition consist of addition of a new phase called Find Phase. The traditional Wi-fi Scan Phase is still used.

1. Find Phase

   The Find Phase is used to ensure that two simultaneously searching P2P Devices arrive on a common channel to enable communication. This is achieved by cycling between states where the P2P Device waits on a fixed channel for Probe Request frames (Listen state) or sends Probe Request frames (Search State) on a fixed list of channels. Convergence of two devices on the same channel is assisted by randomizing the time spent in each cycle of the Listen State. Time to converge is minimized by limiting the list of channels to the Social Channels. In the Find Phase, a P2P Device shall alternate between the Listen and Search states as specified below.

   In case of Wi-Fi Direct, there are dedicated channels used for discovery procedures. These channels are called **Social Channel** and they are channel number 1, 2 and 11 in 2,4 GHz band.

   During the **Listen State**, a P2P Device dwells on a given channel and "listen to" incoming probes in order to answer under specific conditions. The Listen Channel shall be chosen at the beginning of the Device Discovery and shall remain the same until P2P Discovery completes.

   A P2P Device in the Search State shall not reply to Probe Request frames.

   During the Find phase, let us state Device B and A want to communicate and Device B is in Search State.

   - B is in Search State : B sends Probe requests in a channel among the list of social channels.

     The MAC frame sent by B contains information as shown in figure below with:

- **P2P capability Bitmap**: It consists in a description of the P2P Device through bitmaps. New capabilities related to Direct Wi-Fi are provided: Concurrent Operation availability, Cross Connection availability and the Persistent Group availability (more detailed information can be found in Table 13 and Table 14) in annex A.6.
- **Listen Channel**: about the operating class (the frequency band value) and channel number (among channels in Social Channel) on which the P2P Device is in the Listen State during discovery phase.

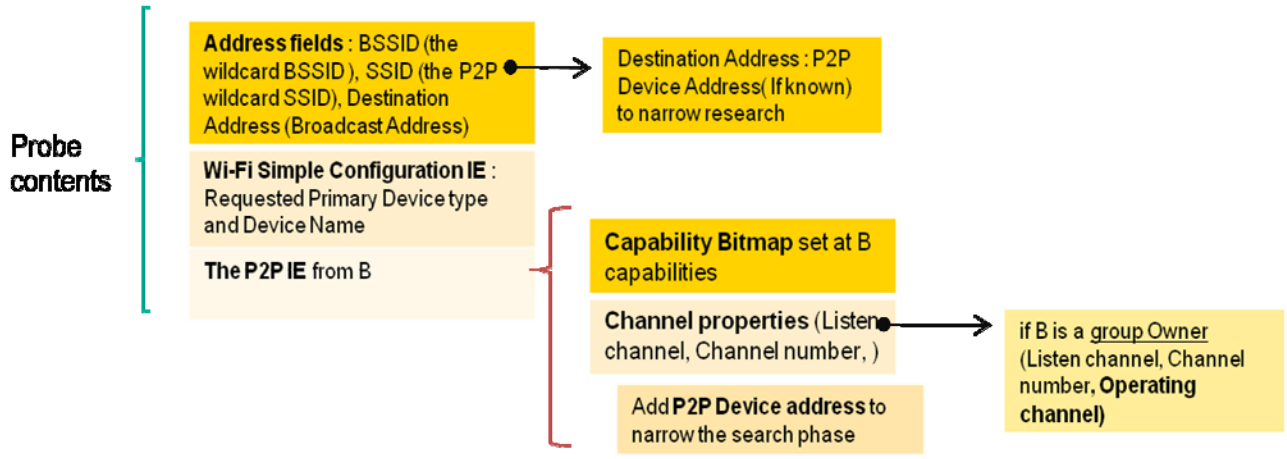


Figure 34 : Probe request content in Direct Wi-Fi

- Device A in listen state will respond only if :
  - It is a Group Owner
  - It is in **Listen state** in the same channel
  - Destination Adress corresponds to its address or is a Broadcast Adress
  - Or it suits the Requested Primary device type or its P2P Device ID is in the received P2P IE

The MAC frame sent by A contains information as in figure belowwith :

- **Device info**: This field includes P2P Capabilities as described previously and other information are available such as Device Name and Device Address. For more information please see Table 15
- **Group Info**: The P2P Group Info attribute contains device information of all P2P Clients that are members of the P2P Group. The information in the Table 16 is given for each device in the group.

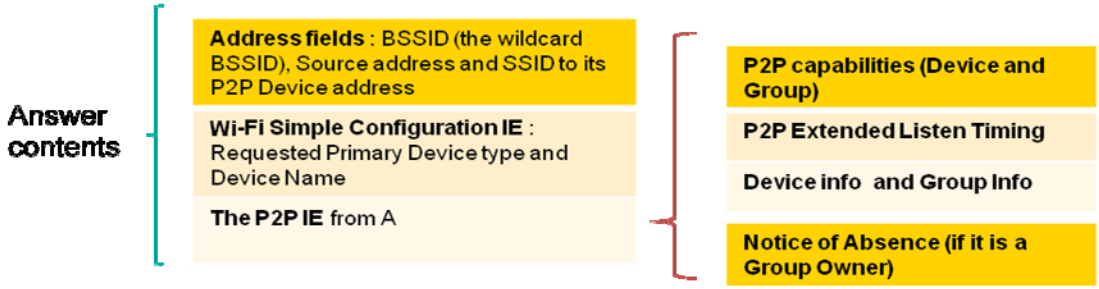


Figure 35 : Probe answer content in Direct Wi-Fi

2. Scan Phase

The Scan Phase uses the scanning process defined in IEEE 802.11 [14]. It may be used by a P2P Device to find P2P Devices or P2P Groups and to locate the best potential Operating Channel to establish a P2P Group. In the Scan Phase, devices collect information about surrounding devices or networks by scanning all supported channels.

Devices in Scan Phase will send Probe requests in all channels and will wait for probe answers. The P2P Device in the Scan Phase shall not reply to Probe Request frames.

A.6.2 Capability bitmaps and Information tables

A.6.2.1 P2P Capability

P2P capabilities are divided into 2 groups : P2P Device Capabilities bitmap and P2P Group Capabilities bitmap.

Information	Service Discoverability	P2P Client Discoverability	Concurrent operations
Description	If sender supports service discovery	If sender supports P2P client discoverability inside a group	If sender supports concurrent operations with other WLAN
P2P Infrastructure manage		**P2P Device Limit**	**P2P Invitation Procedure**
The P2P interface of the P2P Device is capable of being managed by the WLAN (infrastructure network) based on P2P Coexistence Parameters		The P2P Device is unable to participate in additional P2P Groups	If the P2P Device is capable of processing P2P Invitation Procedure signalling

Table 13 : Device Capabilities bitmap

Information	P2P Group Owner	Persistent P2P Group	P2P group limit
Description	If it operates as a GO	If sender intends to host or host a P2P persistent group	If the GO can add another P2P client in its P2P group
Intra-BSS Distribution	**Cross Connection**	**Persistent Reconnect**	**Group Formation**
If the P2P Device is hosting, or intends to host, a P2P Group that provides a data distribution service between Clients in the P2P Group	If the P2P Device is hosting, or intends to host, a P2P Group that provides cross connection between the P2P Group and a WLAN, i.e. Cross connect between a WLAN and a P2P Group using any mechanisms above layer 2	When the P2P Device is hosting, or intends to host, a persistent P2P Group that allows reconnection without user intervention	If the P2P Device is operating as a Group Owner in the Provisioning phase of Group Formation

Table 14 : Group capabilities bitmap

Note : **A P2P Persistent Group** is a P2P Group for which Credentials are stored and may be made available for reuse after the initial use completes

A.6.2.2 P2P Information tables

It can be divided into 2 groups : Device Information and Group Information

WSC stands for Wi-Fi Simple Configuration (technical specifications are not avalaible)

Information	P2P device address	Config method	Primary device type
Description	An identifier used to uniquely reference a P2P Device	The WSC methods that are supported by the device : PIN from a keypad…It contains only the data part of WSC configuration methods attribute	

Number of secondary device types	Secondary device Type list	Device Name
		Friendly name of the P2P Device

Table 15 : Device Information

Note : Primary Device Type, Secondary Device Type definitons are explained in a non-avalaible document. These fields specify the nature of device (computer, network infrastructure, storage, etc.).

Information	P2P device address	P2P Interface Address	Device capability Bitmap	Config method
Description	An identifier used to uniquely reference a P2P Device	An address used to identify a P2P Device within a P2P Group		See Table 6

Table 16 : additional information in Group Information

Note : Table 16 includes shows new elements in Group Information (GI). The whole GI is completed with Device Information elements.

A.7 IEEE 802.21

The IEEE 802.21 “Media-Independent Handover (MIH) Services” standard [15] provides a set of extensible mechanisms mainly targeted to enable the optimization of handovers between heterogeneous IEEE 802 systems as well as facilitate handovers between IEEE 802 systems and cellular systems (e.g., 3GPP and 3GPP2). To that end, the standard defines:

a) A new functional entity (i.e., MIH Function, MIHF) to be allocated within terminals and networks.

b) A set of media-independent and media-dependent interfaces for information exchange between the MIHF entity and other collocated system functional entities (e.g., link and network layer entities).

c) A signalling protocol for message exchanging between remote MIHF entities.

The MIHF entity is intended to have some control on link layer behaviour (e.g., perform link actions such as power-up and link configuration) and manage link layer information gathering (e.g., link status polling or event-triggered information). Information exchange between MIHF entity and link layers is supported by means of media-dependent interfaces for IEEE 802 link-layer technologies (IEEE 802.2, IEEE 802.3, IEEE 802.11, and IEEE 802.16) and cellular technologies (3GPP and 3GPP2). In multi-RAT terminals, a MIHF entity shall have a separate media-dependent interface for each supported radio link layer.

On the other hand, MIHF offers a set of services to entities within upper layers of the protocol stack (denoted as *MIH users* according to 802.21 standard’s terminology). Services provided to MIH users are classified as event, command and information services. Through these services, MIHF facilitates handover decision making to mobility management entities by allowing these (upper layer) entities to control at some extent link layer’s behavior (e.g., perform remote/local link actions and trigger handover commands) and providing them

with useful information for more efficient handover decisions (e.g., local/remote link status and information about different available networks and their services). In this case, MIHF services are provided to MIH users by means of a media-independent interface.

The IEEE 802.21 communication model considers MIH information exchanges between terminals and networks as well as between networks. Aforementioned IEEE 802.21 main elements and the basic communication model are illustrated in Figure 36.

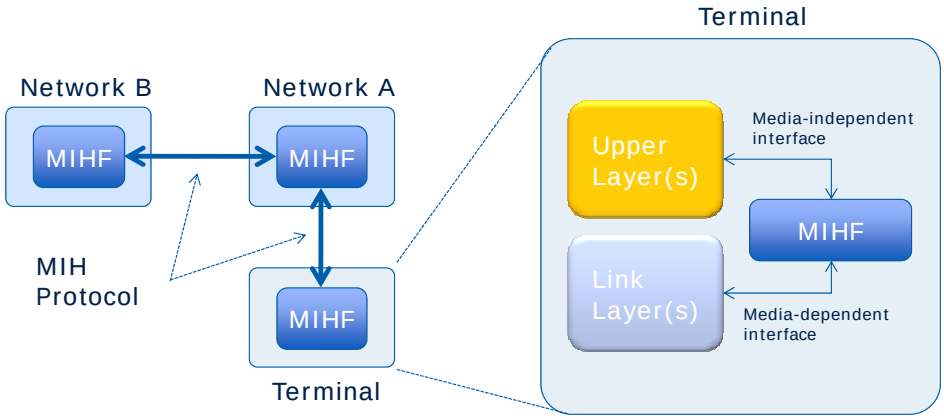


Figure 36: IEEE 802.21 basic communications model and main functional components of IEEE 802.21

The 802.21 service model offers a flexible framework to facilitate different handover approaches. Hence, while served by a given wireless network, the MIHF entity of the mobile terminal could interact with a MIHF entity in the serving network in order to retrieve inter-RAT network information and initiate an inter-technology handover by indicating a preferred list of candidate access networks. As well, handover could also be initiated from the network side. In both cases, 802.21 signalling enables intersystem radio resource availability check and resource preparation (e.g., intersystem resource reservation) between involved networks and provides the terminal with the required configuration of the reserved resources at the target network. It's worth noting that the scope of 802.21 is limited to handover initiation and preparation phases, while the execution phase is not covered (e.g., mobility handling in upper layers is still required for service continuity between networks). Further details about MIH protocol and types of information exchanged between MIH entities are given below.

MIH Protocol

The IEEE 802.21 defines a complete protocol for message exchanges between remote MIH entities whose main characteristics are:

- Transaction oriented. At any given moment, an MIH node shall have no more than one transaction pending for each direction with a certain MIH peer.
- Reliable delivery service, flow control and fragmentation/reassembly. These functions are mainly intended to be used when transport mechanisms available to transfer MIH signaling messages between remote MIH entities do not support such functionalities.

- Each MIHF entity is identified by means of a network access identifier (NAI) that shall be unique as per IETF RFC 4282 (e.g., fully qualified domain name). MIHF identifiers are included in all protocol messages. A multicast MIHF identifier is also defined.
- The protocol supports solicited and unsolicited MIH function discovery and capability discovery procedures.
- Transport-agnostic design: MIH signaling messages can be transferred by means of either layer 2 (L2) or layer 3 (L3) protocols.

As to the transport of MIH signaling:

- Transport over IP networks (i.e., L3 transport) is possible by encapsulating MIH protocol data units within existing transport layer protocols such as TCP, UDP and SCTP (Stream Control Transmission Protocol). In this regard, IETF RFC 5677 [30] specifies mechanisms for MIHF discovery and transport-layer mechanisms for the reliable delivery of MIH messages over IP networks.
- Transport of MIH protocol data units can be supported over any compliant IEEE 802 Std technology (i.e., L2 transport) by using its own protocol identification (e.g., an IEEE assigned *EtherType* value exists for MIH protocol). In addition, as the L2 data plane may not be available for transport before user authentication with the network, both IEEE 802.11 and IEEE 802.16 networks also consider extensions to transfer a limited set of MIH protocol messages before authentication over the management plane by using MAC management frames (e.g., IEEE 802.11u, IEEE 802.16g). On the contrary, 3GPP specifications do not consider so far the transfer of MIH signalling messages on top of RRC signalling protocol.

MIH information types

As to the protocol contents, four types of information can be distinguished attending to the supported MIH service:

- Service management. Service management mainly covers configuration aspects of MIHF entities prior to providing the MIH services from one MIHF to another (e.g., some MIH services are only available under a registration-based approach). Examples of supported procedures are: registration, capability discovery and event subscription.
- Media Independent Event Service (MIES). MIES provides a service to configure event triggering rules and transfer event notifications between MIHF entities. Events indicate changes in state and transmission behaviour of the physical, data link and logical link layers, or predict state changes of these layers. Examples of supported events are: *Link Up/Down/Detected*, *Link Parameters Report*, *Link Going Down*, etc.
- Media Independent Command Service (MICS). MICS provides a service to invoke commands between MIHF entities in order to manage and control link behaviour relevant to handovers and mobility. Examples of supported commands are: *Link Get Parameters*, *Link Configure Thresholds*, handover commands, etc.).
- Media Independent Information Service (MIIS). MIIS is an information service conceived to provide mobile terminals with details on the (static) characteristics and services of the serving and neighboring networks (e.g., network type, operator identifier, frequency bands, etc.). The MIIS service is built on the specification of

various Information Elements (IEs) that can be transferred between remote MIHF entities. The list of IE's specified so far in the standard basically covers: (1)general and access network specific information, (2) point of attachment (PoA) specific information and (3) other information that is access network specific, service specific, vendor/network specific. IEs can be represented by means of two distinct methods specified in the standard: binary representation and Resource Description Framework (RDF) representation that is a general-purpose language for representing information in the Web [38]. Both *get* and *push* modes are supported.

A.8 IEEE P1900

IEEE SCC41 has published in February 2009 the standard IEEE 1900.4-2009 on "IEEE Standard for Architectural Building Blocks Enabling Network-Device Distributed Decision Making for Optimized Radio Resource Usage in Heterogeneous Wireless Access Networks" [19][39]. In this context, a Network Reconfiguration Manager (NRM) is introduced in order to control context and policy provisioning as well as network reconfiguration management; the related information is exchanged via the so-called Radio Enabler and communicated to the Terminal Reconfiguration Manager (TRM) in the various terminal devices. The end-user terminals are multimode terminals, supporting several RATs, with multi-radio link capabilities, as well as with cognitive radio capabilities, such as operating flexibly on different frequency bands. The composite radio access network is assumed to be operated by either a single or several operators. Within this field of application, the standard provides common means to improve overall composite capacity and quality of service through distributed optimization of the usage of spectrum and radio resources offered by the composite radio access network. Basically, the optimization relies on a collaborative information exchange between the composite network and terminals. It should be noted that no explicit transport mechanisms or protocols have been specified for the delivery of pertinent management information. Specifically, the standard introduces an information model at the application layer based on an object-oriented approach addressing a heterogeneous wireless communication framework. Three reference use-cases have been defined within IEEE P1900.4-2009, namely, "Dynamic Spectrum Assignment", "Dynamic Spectrum Sharing", and "Distributed Radio Resource Usage Optimization".

After the publication of the IEEE 1900.4-2009, two projects have started under the scope of P1900.4. Specifically, P1900.4a [19] aims at developing an amendment to IEEE 1900.4-2009 for enabling "Dynamic Spectrum Access Networks in White Space Frequency Bands" by introducing new blocks and new interfaces in the system architecture. The second project, P1900.4.1 [19], aims at specifying the protocols and the Service Access Points (SAPs) present in IEEE 1900.4-2009 System Architecture. The SAPs ensure the interaction between 1900.4 entities and hardware components (terminals or RANs). The protocols are related to the collection of RAN context information and reconfiguration of RANs based on the decision of the NRM; to the collection of terminal context information and reconfiguration of terminals based on the decision of the TRM; to the communication between terminals; and to the communication between Network and Terminal Reconfiguration Managers over the Radio Enabler.

Further activities in the SCC41 committee include work on Policy Languages (P1900.5) [21] and on the definition of interfaces and data structures for dynamic radio systems (P1900.6) [22]. P1900.6 focuses on the interfaces between the sensing and decision making

mechanisms in cognitive radios, cognitive radio systems and in dynamic spectrum systems in general. The P1900.6 working Group aims at developing a “Standard for Spectrum Sensing Interfaces and Data-Structures for Dynamic Spectrum Access and Other Advanced Radio Communication Systems”. The scope of this work is to define the information exchange between spectrum sensors and their clients. These clients may include, in the case of standalone terminals, opportunistic decision making processes, or in more complex larger scale radio communication systems, the radio planning and management mechanisms. The interfaces will be defined to cover both directions of possible interaction; they will be defined as logical interfaces to support the data structures that are used for the information exchange (sensing data, as well as sensing control data). These data structures will be defined abstractly, to avoid any constraining of the sensing technology, the design of the “decision maker” or spectrum manager, nor the type of link between sensor and client. In addition, a range of different sensing techniques have been defined so far, but there has been no effort to ensure interoperability between sensors and clients provided by different manufacturers.

A.9 Distributed Agents for implementation of the CPC concept

Interestingly, JADE (JADEX) and the relevant transport mechanisms (described in section 5.4.4) have been utilized for implementing the CPC concept [52] (following the information model specified in the standardized P1900.4 management architecture [19]). The results obtained from the experimentation and assessment on this JADE–based implementation showed satisfactory behavior in terms of induced signaling loads (number of delivered bytes, bit-rate, overheads imposed by agents’ communication) and time delays, that is equivalent to minimal intervention in the real network operation. Starting from this work, an extended information flow has been defined in the form of an ontology, and an enhanced platform has been developed, also based on JADE, with a special focus on openness, scalability and dynamic extensibility of the platform [53]. Indicative results derived through this platform show that even though there is still some overhead (due to the agent platform) the overall amount of information exchanged (even in situations where there is a large amount of data that needs to be transmitted) is realistic.

A.10 IETF Diameter

The DIAMETER base protocol as defined in IETF RFC 3588 [28] is an extensible protocol to which new building blocks can be added for different applications. One example are extensions used by 3GPP which are defined on a high level in IETF RFC 3589 [29] and in detail in 3GPP TS 29.229 [9].

The original scope of the Diameter base protocol is to provide an Authentication, Authorization and Accounting (AAA) framework for applications such as network access or IP mobility.

Diameter messages shall be transported over SCTP or TCP, typically using the Diameter default port 1812. UDP is supported only for RADIUS backwards compatibility.

Due to the fact that DIAMETER is an easily extensible protocol, extensions can for example be defined for Cognitive Management Procedures or for accessing Dynamic Spectrum Management (DSM) information.

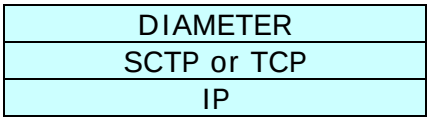


Figure 37: Diameter Protocol Stack

A.11 Broadband Forum TR-069

The Technical Report TR-069 "CPE WAN Management Protocol (CWMP)"[36] is a technical specification from the Broadband Forum (which was earlier called DSL Forum)[35].

The TR-069 is a protocol for communication between a CPE and Auto-Configuration Server (ACS) that encompasses secure auto-configuration as well as other CPE management functions within a common framework. This protocol leveraged SOAP RPC web services to define a firewall friendly management protocol that is highly accepted by the industry.

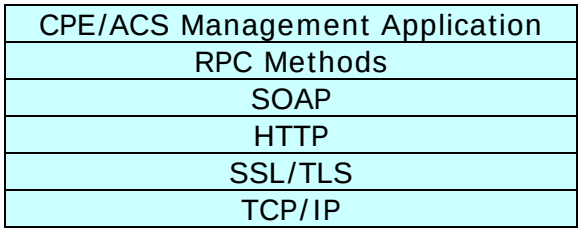


Figure 38: TR-069 Protocol Stack

The TR-069 is used not only for the management of DSL-routers but also in 3GPP for the configuration of Home Node B`s and Home Node B Gateways[10].

A.12 IEEE 802.19

A.12.1 Scope

The standard specifies radio technology independent methods for coexistence among dissimilar or independently operated TV Band Device (TVBD) networks and dissimilar TV Band Devices. The aim of the standard is to enable the family of IEEE 802 Wireless Standards to most effectively use TV White Spaces by providing standard coexistence methods among dissimilar or independently operated TVBD networks and dissimilar TVBDs. This standard addresses coexistence for IEEE 802 networks and devices and will also be useful for non IEEE 802 networks and TVBDs. When completed, these methods will be useful for cognitive systems, especially the ones which are going to operate in the TV White Spaces.

Various deployment options to facilitate coexistence are being considered, where a separate TVWS database would be maintained in each case, which communicates with the Coexistence Enabler for each TVBD network. In one of the deployment options considered, a separate coexistence database and a coexistence management server (or simply the coexistence manager) is also introduced, which aid the coexistence enablers and TVWS database to decide which white space to allot to which TVBD network. This system architecture supports both centralized and distributed decision making. Some Coexistence Reconfiguration Parameters have been proposed, which can be modified to increase coexistence between networks or devices. These include Operating channel, Maximum Transmit Power, Modulation and Coding Rate (Spectral efficiency), Bandwidth, Transmit

Scheduling, CSMA parameters, Transmit Duty Cycle Limit, OFDMA Uplink client sub-band, Spatial parameters.

A.12.2 System Architecture

The 802.19.1 System has 6 logical entities and 6 logical interfaces [15]. Each 802.19.1 logical entity is defined by its functional roles and interfaces with other 802.19.1 logical entities. 802.19.1 Logical entities are composed of 3 internal entities and 3 external entities as depicted in figure 1. The internal logical entities are:

- Coexistence Manager (CM)
- Coexistence Enabler (CE)
- Coexistence Discovery and Information Server (CDIS)

The coexistence manager (CM) has a responsibility for coexistence decision making to facilitate coexistence problems between TV band device (TVBD) networks or devices. It generates and provides corresponding coexistence requests/commands and control information to coexistence enablers. It discovers/communicates with other neighbour coexistence managers to collaborate with them, to solve coexistence problems between multiple coexistence managers with TVBD networks or devices they are engaged. It also assists network operators in management related to TVWS coexistence. The coexistence manager is located inside or outside TVDB.

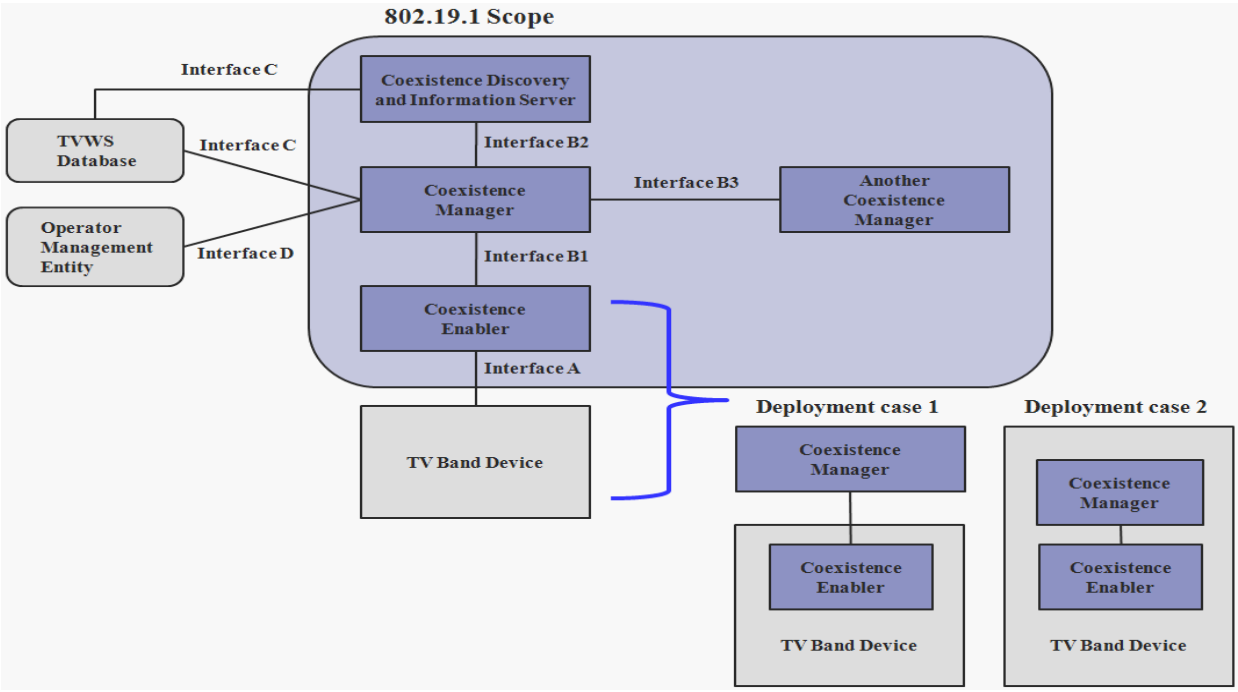


Figure 39: 802.19.1 System architecture [15]

The coexistence enabler (CE) has a responsibility for the communication between coexistence manager and TVBD. It requests/obtains information required for coexistence from TVBD. It also translates reconfiguration requests/commands and control information received from the coexistence manager into TVBD-specific reconfiguration

requests/commands and sends them to the TVBD. The coexistence enabler should be located inside the TVBD.

The coexistence discovery and information server (CDIS) supports discovery of other coexistence managers and opens interfaces between coexistence managers to provide coexistence related information exchange among coexistence managers. It collects/aggregates coexistence related information from multiple coexistence managers. It also communicates with the TVWS database to obtain information on incumbents.

A.12.2.1 Interfaces

The external logical entities are as follows:

- TVBD network or device
- TVWS database TVWS DB
- Operator management entity (OME)

TVBD or TVBD network is the device or network, which operates with unlicensed basis in the TV bands at locations where that TV bands are not being used by any incumbents, i.e., licensed services. The TVWS database is the regulatory database which provides list of disallowed channels for TVBD networks or devices because they are occupied by incumbents. The operator management entity provides operator related information for coexistence. TVWS database and operator management entity are out of scope of this standard.

The six logical interfaces are:

- Interfaces between 802.19.1 entities
  - Interface B1
  - Interface B2
  - Interface B3
- Interfaces between an 802.19.1 entity and TVBD
  - Interface A
- Interfaces between 802.19.1 entities and TVWD database or OME
  - Interface C
  - Interface D

Different interfaces between 802.19.1 logical entities are distinguished by their usage, types of information exchanged, and underlying protocols.

A.12.3 Reference Use Cases

Coexistence problems between TVBD networks or devices might occur due to the disparity between the number of available channels and the number required operating channels for TVBD networks or devices over a given area. One operating channel might consist of one or more TV channels based on the demand of each TVBD network, e.g., 10MHz channel bandwidth can be supported by two consecutive 6MHz TV channels in U.S.A or two consecutive 8 MHz channels in Europe.

There might be three different patterns of allocating operating channels to TVBD networks as follows;

- To allocate a free and unoccupied channel to each TVBD network
- To allocate a free and unoccupied channel to two or more TVBD networks at the same time
- To allocate a pre-occupied channel by one TVBD network to another TVBD networks

For the first case each TVBD network can use an operating channel alone. For the second and third case one TVBD network should share the same operating channel with another TVBD network. The following two use cases are defined within this standard as depicted in figure 2:

- Individual channel assignment
- Co-channel sharing

In the individual channel assignment use case, available channels are dynamically assigned to each TVBD network which has a different operating channel. So it is possible that non-overlapped operating channel among allocated channels for TVBD networks. This guarantee co-channel-interference-free channel use and coexistence problem can be eliminated through a proper channel allocation. In co-channel sharing use case, two or more TVBD networks share the same channel as an operating channel. There could exist a number of operating channels that are being shared. The same operating channel causes co-channel interference:

- An operating channel sharing with the same TVBD networks; Self-coexistence mechanism might be needed to mitigate co-channel interference.
- An operating channel sharing with dissimilar TVBD networks; Inter-system coexistence mechanism might be needed to mitigate co-channel interference.

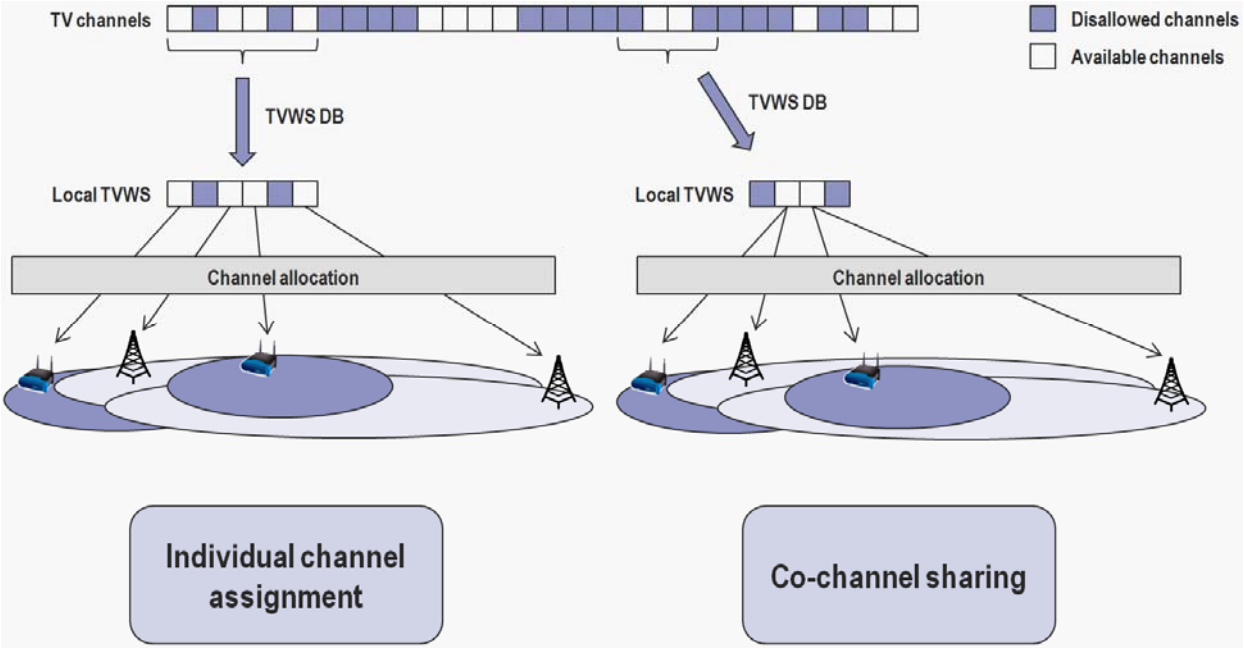


Figure 40: 802.19.1 Reference use cases [15]

A.12.4 Reference Model

Figure 3 shows the 802.19.1 reference model. 802.19.1 entities are located on the application layer. Each 802.19.1 entity has one or more the following service access point (SAP):

- CX_DME_SAP (CoeXistence Device Management Entity SAP): to communicate with TVBD management entities, e.g., 802.11 SME, 802.22 NCMS
- CX_NET_SAP (CoeXistence NETwork SAP): to communicate with remote "802.19.1 internal entities" (CE/CM/CDIS) or OME or TVWS DB

CE shall have

- CX_DME_SAP: to communicate with TVBD management entities
- CX_NET_SAP: to communicate with remote CM

CM/CDIS shall have

- CX_NET_SAP: to communicate with remote 802.19.1 internal entities or OME or TVWS DB

TVBD management entity shall provide CXPM (coexistence primitive mapping) service. CXPM converts CX_DME_SAP primitives into TVBD-specific management/control primitives. 1-to-1 mapping might be highly desirable to fully support 802.19.1 standard, but it might depend upon the degree of modification of each TVDB standard. How to implement CXPM is out of scope of the standard.

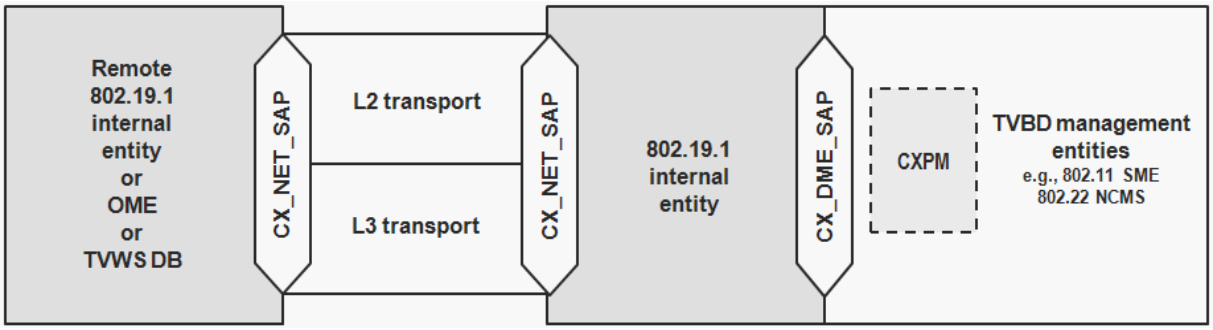


Figure 41: 802.19.1 Reference model [15]

A.13 3GPP E-UTRAN Protocol Stack Overview

When work on 3GPP Rel-8 started, 3GPP made an effort to specify an evolved UTRAN system (E-UTRAN). This endeavour is commonly known under the term LTE (Long Term Evolution). The Base Stations of the E-UTRAN system are called eNodeBs. An eNodeB of the E-UTRAN is more intelligent than a legacy NodeB of a UTRAN system, as almost all the RNC functionality has been moved to the eNodeB. Figure 42 shows an example E-UTRAN architecture comprising three eNodeBs. In E-UTRAN eNodeBs are interconnected with each other by means of the X2 interface (red lines in Figure 42). Furthermore eNodeBs are connected by means of the S1 interface (green lines in Figure 42) to the EPC (Evolved Packet Core). The S1 interface as defined by 3GPP supports a many-to-many relation between EPC and eNodeB, i.e. the standard allows for simultaneous operation of an eNodeB by different operators.

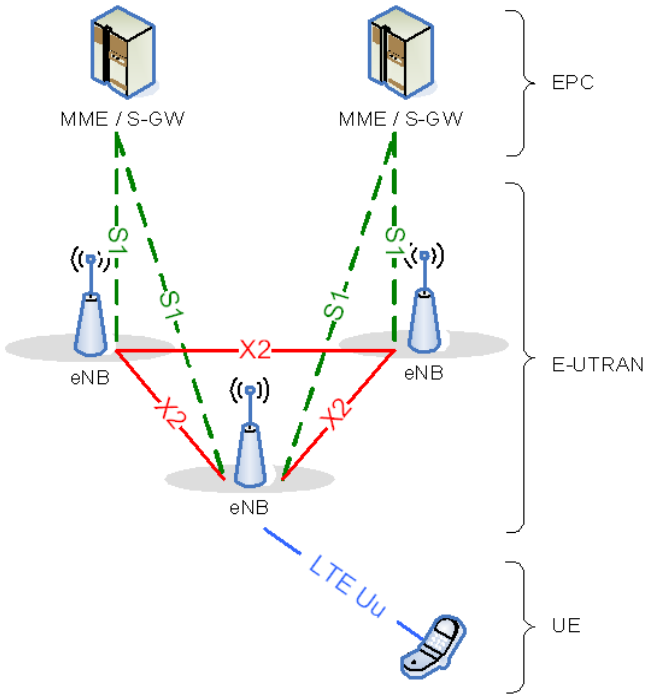


Figure 42: EPC elements, E-UTRAN, and UE are forming the LTE Communication System.

Figure 43gives an overview of the protocol stack for the E-UTRAN air interface. The bottommost layer is the physical layer (Layer 1). Layer 2 is split into the following sublayers: Medium Access Control (MAC), Radio Link Control (RLC) and Packet Data Convergence Protocol (PDCP). The Service Access Points (SAP) between the physical layer and the MAC sublayer provide the transport channels. The SAPs between the MAC sublayer and the RLC sublayer provide the logical channels. The multiplexing of several logical channels on the same transport channel (i.e. transport block) is performed by the MAC sublayer. In both uplink and downlink, only one transport block is generated per TTI in the non-MIMO case. The LTE protocol stack can not only be divided horizontally as described above, but also vertically into a control plane (c-plane) and a user data plane (u-plane) as shown in Figure 5. The RRC protocol layer making up the c-plane of the E-UTRAN air interface is of particular relevance for the OneFIT findings, because at this level control information is exchanged between the mobile node and the base station and (by using the piggybacking function of the RRC Messages for NAS messages) also between the mobile node and the EPC (direct UL/DL message transfer). In the following text the term User Equipment (UE) denotes the mobile node. The main services and functions of the RRC layer include:

- Broadcast of System Information (SI) related to the non-access stratum (NAS),
- Broadcast of System Information (SI) related to the access stratum (AS),
- Paging,
- Establishment, modification and release of an RRC connection between the UE and E-UTRAN including:
    - Allocation of temporary identifiers between UE and E-UTRAN;
    - Configuration of signalling radio bearer(s) for RRC connection:

- Low priority SRB and high priority SRB.

- Security functions including key management,
- Establishment, configuration, maintenance and release of point-to-point Radio Bearers,
- Mobility functions including:
- UE measurement reporting and control of the reporting for inter-cell and inter-RAT mobility;
  - Handover;
  - UE cell selection and reselection and control of cell selection and reselection;
  - Context transfer at handover.
- Notification for MBMS services,
- Establishment, configuration, maintenance and release of Radio Bearers for MBMS services,
- QoS management functions,
- UE measurement reporting and control of the reporting,
- NAS direct message transfer to/from NAS from/to UE.

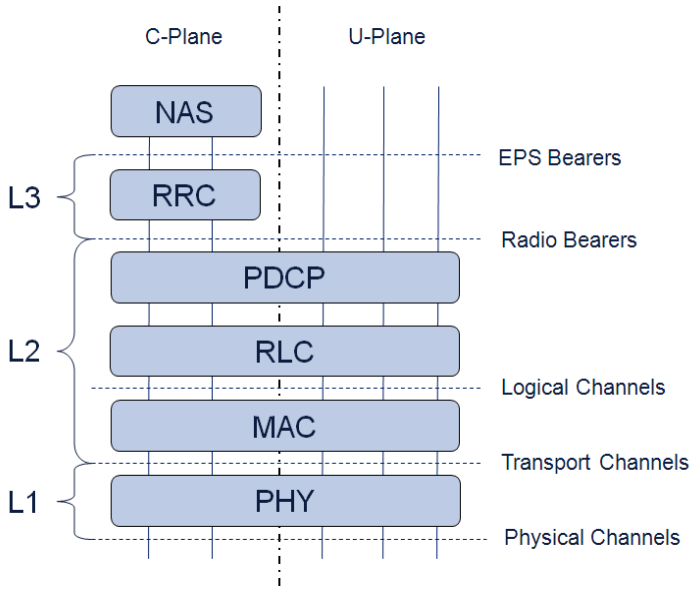


Figure 43: Protocol Stack overview for the air interface of the 3GPP LTE system

NAS Direct Message Transfer

Below a summary of the direct UL/DL message transfer methods is given as defined in the LTE RRC specification TS 36.331:

The DLInformationTransfer message is used for the downlink transfer of dedicated NAS information.

- Signalling radio bearer: SRB2 or SRB1 (only if SRB2 not established yet. If SRB2 is suspended, E-UTRAN does not send this message until SRB2 is resumed.)
- RLC-SAP: AM
- Logical channel: DCCH
- Direction: E-UTRAN to UE

The ULInformationTransfer message is used for the uplink transfer of dedicated NAS information.

- Signalling radio bearer: SRB2 or SRB1(only if SRB2 not established yet). If SRB2 is suspended, the UE does not send this message until SRB2 is resumed
- RLC-SAP: AM
- Logical channel: DCCH
- Direction: UE to E-UTRAN

Signaling Radio Bearers

SRBs are defined as Radio Bearers (RB) that are used only for the transmission of RRC and NAS messages. More specifically, the following three SRBs are defined:

- SRB0 is for RRC messages using the CCCH logical channel (= Common Control Channel);
- SRB1 is for RRC messages (which may include a piggybacked NAS message) as well as for NAS messages prior to the establishment of SRB2, all using DCCH logical channel (= Dedicated Control Channel);
- SRB2 is for NAS messages, using DCCH logical channel. SRB2 has a lower-priority than SRB1 and is always configured by E-UTRAN after security activation.

In downlink direction piggybacking of NAS messages is used only for one of the following procedures: bearer establishment/ modification/ release. In uplink direction NAS message piggybacking is used only for transferring the initial NAS message during connection setup. The NAS messages transferred via SRB2 are also contained in RRC messages, which however do not include any RRC protocol control information. Once security is activated, all RRC messages on SRB1 and SRB2, including those containing NAS or non-3GPP messages, are integrity protected and ciphered by PDCP. NAS may choose to independently apply integrity protection and ciphering to the NAS messages at NAS level.

A.14 3GPP E-UTRAN States

The RRC (Radio Resource Control) protocol defined for E-UTRAN uses the following states: RRC_CONNECTED and RRC_IDLE. A UE is in RRC_CONNECTED when an RRC connection has been established between the UE and the (H)eNB. Otherwise it is residing in RRC_IDLE state. The RRC states can further be characterised as follows:

- RRC_IDLE:
    - Mobility is controlled by the UE (cell re-selection);
    - The UE:
        - Monitors a Paging channel to detect incoming calls and System Information (SI) change;
        - Performs neighbouring cell measurements and cell (re-)selection;

        - Acquires System Information (SI).
- RRC_CONNECTED:
    - Transfer of unicast data to/from UE (dedicated message transfer).
    - Mobility is controlled by the network (handover and cell change order);
    - The UE:
        - Monitors a paging channel and/or System Information Block Type 1 (SIB-Type1) contents to detect System Information (SI) change;
        - Monitors control channels associated with the shared data channel to determine if data is scheduled for it
        - Provides channel quality and feedback information;
        - Performs neighbouring cell measurements and measurement reporting;
        - Acquires System Information (SI).